FP7-SEC-2011-284725

SURVEILLE

Surveillance: Ethical Issues, Legal Limitations, and Efficiency
Collaborative Project

SURVEILLE Deliverable 2.2: Paper with Input from End Users

Due date of deliverable: 28.02.2013
Actual submission date: 28.02.2013

Start date of project: 1.2.2012 Duration: 39 months

SURVEILLE Work Package number and lead: WP02 Prof. Tom Sorell
Author(s): Dr. John Guelke

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)	

Executive Summary

1. The earlier FP7 project DETECTER project constructed a normative framework for considering the ethical risks of surveillance technologies in counter-terrorism investigations.
2. This is compared with a new framework devised for normative assessments extracted from submissions by the SURVEILLE End User Panel of 45 surveillance technology products presented in SURVEILLE deliverable D2.1.
3. Although there is substantial overlap, ethical risks of surveillance in SURVEILLE arise from a wider range of situations than terrorism which was in focus for DETECTER.
4. The normative grounding for ethical risk is considered in relation to five possible features of serious crime: significant financial loss to the victim, use of violence, threat to public order, organisation, and significant financial gain for the perpetrator.

1. The DETECTER Normative Framework

The DETECTER project[1] analysed the ethical and legal norms of the use of detection technology in counter-terrorism investigations. WP02[2] and WP03,[3] on detection technology review and the ethical norms of counter-terrorism respectively, developed a framework of ethical analysis that serves as a useful basis for

[1] http://detecter.eu/

[2] See, for example: D12.2.10 'Detection Technology Quarterly Update 10' www.detecter.bham.ac.uk/pdfs/D12_2_10_QuarterlyUpdateonTechnology_10__1_.doc

[3] See in particular: D5.1 'The Moral Risks of Preventive Policing' http://www.detecter.bham.ac.uk/pdfs/D05.1MoralRisksofPreventivePolicingv2.pdf,

D5.2 'The Relative Moral Risks of Detection Technology' www.detecter.bham.ac.uk/pdfs/D05.2.The_Relative_Moral_Risks_of_Detection_Technology.doc and

D5.3. 'Taking Moral Risks Given an Analysis of what's Wrong with Terrorism' www.detecter.bham.ac.uk/pdfs/D05.3.TakingMoralRisksv2.doc

considering the ethical norms of use of surveillance technology in serious crime more generally. In section 1 I outline this framework.

The DETECTER project identified three distinct categories of harm of detection technologies: intrusion, error and damage to trust. Intrusion is understood in terms of penetration of a normatively protected zone of a person or their life. Normatively protected zones of privacy are breached by looking uninvited into a changing room, or by looking uninvited through somebody's correspondence.

At least three categories of normative protection associated with the concept of privacy can be identified. This is normative in the same sense that there are normatively sustained conventions against lying – normative protections in this sense are quite distinct from legal protections. The norms of privacy in question include the following: respect for bodily privacy, particularly the privacy of the naked body; respect for privacy of home spaces; and finally respect for private life – matters of conscience and association understood to be private matters even when pursued in public places such as places of worship or libraries.

Surveillance technologies may intrude on bodily privacy when they scan the body directly, as is the case with certain radar scanners and millimetre wave full body scanners. Bodily privacy may also be intruded upon by video or audio technologies if they are placed in areas such as changing rooms which are widely understood as being protected from observation.

Likewise, homes are widely understood as protected from others' observation. The home is the place that one has greatest latitude to do as one pleases without the scrutiny or interference of others. Hotel rooms can take on a similar (albeit temporary) significance for a guest occupying them, and thus bugs or miniaturised cameras placed in such places can be highly intrusive in the same way as if they were placed in the home.

We additionally have a concept of 'private life' that covers much of the life that is led outside the home; for example, when one arranges to go to a restaurant with a romantic partner or attend a meeting of a local religious organisation in a place of worship explicitly open to all, such activities may reasonably be thought part of one's private life. This is a weaker form of privacy, and cannot rule out all observation – after all one might not be able to help seeing a couple at dinner in a restaurant if one is dining there oneself. However, it does rule out persistent attention, eavesdropping or following as intrusive behaviour in need of justification. Technologies can penetrate the privacy of private life by virtue of their ability to track an individual's movements and activity. Furthermore, bugging and telephone taps are intrusive in part because of what they reveal about the individual's private life.

Intrusion is not the only significant ethical risk associated with detection and surveillance technologies. Errors may be harmful when they lead to false arrest or harassment. The most extreme consequences of error, such as miscarriage of justice, are arguably even more significant than the most extreme intrusions. However, the intention is not comparison between the different categories of risk. The framework is intended to identify the different kinds of ethical danger that determine the overall riskiness of different techniques, technologies and investigations. Investigations invariably pose some risk of error, of false suspicion and inconvenience to innocent people. However, certain kinds of investigation and especially, for example, those in preventive counter-terrorism are particularly prone to the false identification of suspects, because there is often very little evidence to rely upon.[4]

[4] Which may well combine disastrously with a high public demand for prosecution – see, for example:(Adam Roberts, 1989, 60) "Its main problems arise from the fact that it involves trying to combat clandestine fighters, who may cause the most appalling carnage, but who hide among the rest of the population and are very difficult to track down. This creates a situation where there is often a strong public desire for retribution, but the proper target for such retribution is not available."

There has been much public coverage of databases of existing suspects and data mining programmes used to identify terrorist suspects.[5] Much public criticism of these techniques has called attention to their intrusiveness,[6] but the large scope for error seems to be the matter of greater concern. Both databases and data mining may be error prone due to problems of name matching (identifying intelligence in a database with a named individual),[7] and data mining techniques often generate many false matches, particularly in the counter-terrorism context.[8]

The injustice of discrimination overlaps with the moral risk of error, as it can be both a cause and an effect of error. It is a cause of error if an individual incorrectly identifies someone as a suspect due to their own discrimination. Discrimination may also be an effect of error if error resulting from a technical or management process systematically casts suspicion on a particular category of person. For example, a number of smart camera systems trigger alerts at what is categorised as 'abnormal activity'[9] – if this systematically identifies innocuous activity on the part of a particular ethnic minority as 'abnormal', and they are repeatedly stopped and questioned as a result, then this is discriminatory.

---

[5] See, for example: http://www.nytimes.com/2008/10/08/washington/08data.html?_r=0 and http://www.guardian.co.uk/uk/2009/feb/25/database-state-ippr-paper, and http://www.aclu.org/technology-and-liberty/feature-capps-ii.

[6] See, for example: Tavani, 1999.

[7] See for example the DETECTER Deliverable D5.2 "Misspellings, spelling variations among phonetically identical names (e.g. Jeff and Geoff), the lack of any standard representation of names from a number of languages that do not use the Roman alphabet, the use of nick names, titles, permutations, abbreviations and omissions of names (which vary by culture), the use of definite descriptions (e.g. 'the Prime Minister of Great Britain' vs. 'Tony Blair') and name changes over time all provide sources of error which may result in unjust sanction" and Branting, L. Karl. 2005, 'Name Matching in Law Enforcement and Counter-Terrorism'

[8] As, for example, notoriously with the German 'Rasterfahndung', identifying suspects by having come from an Islamic country, 'being registered as a student', and being a male between 18 and 40 years of age. The system identified 300, 000 individuals, and resulted in no arrests or prosecutions. On a range of other counter-terrorism data mining programmes see DETECTER Deliverable D8.1. www.detecter.bham.ac.uk/pdfs/D8.1CounterTerrorismDataMining.doc

[9] See, for example: Behavioural Recognition Systems' AIsight 2.1 http://www.brslabs.com/files/pdf/AISight_2%201_Final.pdf.

However, discrimination is more than this. Discrimination is an injustice that results from treating factors about a person as relevant to criminality when they are not. Discrimination usually also involves inconsistency in the treatment of these factors. This inconsistently treats clothing or features to do with a person's identity as evidence of likely behaviour. For example, treating a person's ethnicity as relevant to the likelihood of membership of a terrorist group. Discrimination is considered ethically wrong both because of the injustice it may lead to and also as an injustice in itself, as reflected in human rights law[10] and a number of European legal institutions.[11]

Moving on to the final category of ethical risk, two valuable kinds of trust may be damaged through the use of detection technologies. The first is trust in policing authorities. Acknowledging this as a risk of surveillance technologies takes account of the damage that overbearing surveillance has had, particularly in previous counter-terrorism campaigns.[12] Indeed, an unfortunate legacy of past illiberal policing practices can be a low level of support for, and an attitude of suspicion towards, police in some communities.[13] The other category of valuable trust that may be undermined is the generalised associational trust of a democratic society. This covers the phenomenon referred to as the 'chilling effect' – disincentivising engagement in political and other associational activity.[14]

[10] See Moeckli (2008) *Human Rights and Non-Discrimination in the 'War on Terror'* p.74

[11] For example the European Parliament's 2009 *Recommendation on the Problem of Profiling*.

[12] See, for example: Paddy Hillyard, 1993, *Suspect Community*; (Pantazis and Pemberton, 2009); (Spalek, El Awa and McDonald, 2008) and Richard English. 2009. *Terrorism: How to Respond* p 141

[13] An extreme example is provided by the fate of policing in post-Apartheid South Africa, where it is argued that the police have very limited legitimacy to operate; see for example Jonny Steinberg's (2009) *Thin Blue* where he argues that this and similar cases show that a population cannot be policed against its will.

[14] See, for example: (DeCew, 1997, 64) on weakening of associational bonds, contributing to "wariness, self-consciousness, suspicion, tentativeness in relations with others".

There are many cases where using risky technology in either preventive or reactive investigations will be justified. DETECTER considered the use of surveillance technology specifically in the case of counter-terrorism. In countering terrorism, three key factors – threats to life, public order, and critical infrastructure – are the basis for overcoming the strong presumption against ethically risky investigative methods. Each threat is normatively significant because of the importance of life, public order and the benefits of critical infrastructure to human welfare.

Protecting the lives of citizens may be the most basic function of government. Life is a condition of any kind of human welfare at all. This obligation on the part of government is primary and overriding when it comes into conflict with other obligations. Threats to life also threaten welfare by virtue of the fear and panic they may cause. This disutility is also relevant to the second feature of terrorism. Maintenance of social order is a basic function of government, a fact reflected throughout most classical political philosophy on the foundations of state authority.[15] Even when life is safeguarded, much of human welfare, and certainly the possibility of having and plausibly pursuing a life plan is contingent on a stable social order.[16] By the same token, the functioning of modern states is highly dependent on the secure functioning of critical infrastructure. Acknowledging the significance of critical infrastructure is important because of the likelihood that damage to it could threaten both life and social order. However, damage to infrastructure that falls short of threatening life or social order could still have a high enough impact on welfare to justify riskier methods of surveillance.

A simplified version of the DETECTER normative framework was presented in a series of technology quarterly updates throughout that project, using a table to represent the relative moral risks of different surveillance technologies. This table is presented

[15] Whether securing peace and order are seen as the primary source of state authority, as in Hobbes and in Kant, or simply because maintenance of order is seen as indispensable to preserving rights as in Locke.

[16] On the central role of 'life plans' in liberal political thought see John Rawls (1971) *A Theory of Justice* section 63.

in Figure 1. Blank text indicated no ethical risk, green a moderate or low risk, yellow an intermediate or medium risk, and red a severe or high risk. This makes clear the framework's suggestion, for example, that data mining techniques are ethically problematic because of their likelihood to generate error and cast false suspicion, rather than because of their inherent intrusiveness, while severely intrusive techniques such as telephone tapping are less likely to cause this problem. It also judged substance detectors across the board as only mildly risky, whereas internet monitoring was found to be severely problematic in all respects.

Overview			
	Intrusion	Error and discrimination	Trust and Chill[17]
CCTV in public places	Mostly only mildly intrusive. Use of smart cameras may be more so.	Possibility for errors.	Because use is widespread, widely known about and there is perception of function creep, the use of CCTV may have significant impacts on trust in the police and political participation.
Covert Bugging	Very intrusive.	Potential for ambiguity and misunderstanding due to context dependence of understanding by third parties.	Although where discovered the intrusiveness of such measures are likely to weaken trust, they are more likely to remain secret and unknown to the public.
Phone Monitoring			
Covert Cameras		Potential for ambiguity.	
Full Body Scanners	Very intrusive if outputting intimate visual image. If less detailed image outputted, or process is automated, intrusion greatly reduced.	Possibility of false positives, but unlikely to result in lasting errors.	Where intrusive scanners are made mandatory as a condition of flight, this is likely to weaken trust in authorities and have a 'chilling effect'. This is greatly reduced by offering alternatives or using less intrusive scanners.
Substance Detectors	Although scans of the body can be considered an invasion of bodily privacy, where this detects only the presence of substances this is a mild	Possibility of false positives, but unlikely to result in lasting errors.	Use likely to be seen as legitimate intrusion by authorities.

[17] The ethical risk summarized as 'trust and chill' refers to both danger of damage to trust in policing authorities and damage to association trust referred to by 'the chilling effect'. For further details see DETECTER Deliverable D5.2 www.detecter.bham.ac.uk/pdfs/D05.2.The_Relative_Moral_Risks_of_Detection_Technology.doc

	intrusion.		
Databases and Data Mining	Only intrusive if information collected is intimate or sensitive in a way that penetrates the sphere of privacy, or reveals such information as a result of aggregation. Otherwise unintrusive.	False information can endure for long periods of time without adequate opportunity for correction. Datamining is at great risk of casting suspicion on large numbers of innocent people, often disproportionately affecting social and cultural groups.	Damaging to trust in the authorities if it is understood to result in sanction for innocent people, especially so if members of 'suspect communities' are disproportionately likely to be victims.
Location Tracking	Potential for intrusion into private life with the exception of emergency calls.	Potential for misjudging the significance of visiting certain places.	To the extent that its use is known about, likely to weaken trust in authorities and chill political participation.
Internet Monitoring	Very intrusive into private life.	Great potential for misjudging the significance of visiting certain websites.	Awareness of internet monitoring is likely to have a severe impact on people's willingness to seek out information on certain topics.

Figure 1: Table of Technologies and moral risks from DETECTER Deliverable D12.2.10 (blank text indicating no ethical risk, green a low risk, yellow medium and red high).

2. End User Panel assessments of Moral Risk for SURVEILLE

SURVEILLE considers a wider range of technologies than were surveyed in DETECTER, and the categorisation of technologies is different. Even more significantly, SURVEILLE considers a broad range of serious crime rather than just terrorism. An appropriate ethical framework for the use of surveillance technology must accommodate these differences.

The SURVEILLE project is assisted in this task by input from the End User Panel (EUP). The EUP consists of senior police officers from across Europe, assembled to provide end user expertise throughout the SURVEILLE project. For the purposes of WP2 – 'Survey of Surveillance Technologies' – their views were sought on 45 technology products, identified and discussed in SURVEILLE Deliverable D2.1.[18] Judgments were solicited on a number of points, including categories of crime for which the product is mainly used, effectiveness and cost effectiveness.[19] They were not requested to

[18] Available at: http://www.surveille.eu/PDFs/D2.1%20Survey%20of%20Surveillance%20technologies.pdf

[19] The questions, in full, were:

do so on the basis of any theoretical or empirical 'method', but rather to make such assessments "in the light of their own jurisdictional experience".[20]

For the purposes of this paper it is the views relevant to the normative framework that are of interest. These views were expressed in their answers to two questions: 'Any significant legal/ethical issues?' and 'View regarding level of intrusiveness – high, medium, low, cannot determine'. The completed worksheets are attached in full in Annex 1. In order to illustrate similarities and differences with the normative framework presented in DETECTER, an overview of their answers to the normative questions are presented in Figure 2. For example the DETECTER framework and the EUP assessments agree that telephone taps and bugging are highly intrusive. They agree substantially on the low intrusiveness of what DETECTER called 'substance detectors' – chemical, biological and radioactive technologies in the SURVEILLE categories, though the DETECTER framework is slightly more permissive, assessing the ethical risks as moderate across the board, while the EUP assessments emphasised that a lack of awareness on the part of the subject could deepen the intrusion, rating covert use of these technologies 'medium'.

There are two main points of disagreement. Millimetre wave full body scanners are treated as more intrusive on the DETECTER view, unless constructed such that the intimate visual image of the body is dispensed with in favour of products which output a non intimate 'stickman' image that merely highlights points on the body where further searches are required. Data mining and profiling technologies are

---

- What category of serious crime does the technology impact on?
- Comment regarding claim as to use by developer.
- Is the technology capable of use in Law Enforcement Agency (LEA) work regarding prevention, intelligence, proactive / reactive detection – (or both).
- Is the technology capable of use in overt / covert investigation or both?
- Assessment as to effectiveness i.e. Significant / of benefit / minimal / unknown / indeterminable? (EUP members to go to Website / if no Website details available MERPOL to refer back to Delft for further details if necessary)
- Any significant legal / ethical issues?
- EUP view regarding level of intrusiveness – high, medium, low, cannot determine.
- EUP view regarding cost effectiveness of equipment?
- Any other comments?

[20] In correspondence with the EUP.

identified as morally problematic in the DETECTER framework, but for different reasons. The DETECTER framework finds data mining and profiling technologies objectionable because they may too easily lead to error and discrimination – a reason not directly considered in the EUP assessments. On the matter of their intrusiveness, both approaches assess their risk as medium.

Technology	Intrusiveness	Ethical/legal issues
CCTV	Dependent on use: Overt – low Covert – medium to high depending on where deployed	Overt positioning of CCTV equipment by public bodies, and in private and commercial locations is widespread. This is regularly advertised and within the knowledge of individuals and the public at large. Covert use of CCTV poses a different aspect and falls into two broad categories: Deployment and use of equipment by a law enforcement agency as part of their activities relating to intelligence, proactive or reactive investigative responsibilities or, Covert use of overtly placed CCTV equipment by LEAs for the proactive surveillance of individuals. There will also be legal and ethical considerations relating to use of overt or covert CCTV equipment that is used to monitor activity in private premises. In reactive investigation (post incident) the use of CCTV from all overt sources should pose little or no legal / ethical issues subject to a LEA's seizure and retention procedures being appropriate. The specific deployment of CCTV equipment for a covert use by a LEA, together with the targeted (and thereby covert) use of overt systems by a LEA should be subject of the appropriate level of authorisation to ensure justification, proportionality and necessity.
Image Processing	Low	If the software conducts analysis of crowds and not individuals, from the information available it would appear that there are no major legal or ethical issues. However, in some EU member states there maybe potential for legal issues in case of use in context of monitoring public assembly (Germany)
Infra Red – motion detector	Low	None – if used in process referred to – single item use.
Radar – short range	Low	None – if used in process referred to – single item use
Radar – acoustic	Low/medium	Minimal if the equipment is used to alert/locate gunfire and differentiate between other sounds (vehicular). With regard to locating people no major issues if detecting trespassers. However, covertly locating individuals would increase the legal and ethical issues and would require the appropriate authorisation.
Radar – array based concealed weapon detection	Low	No legal issues. Pre requirement for flights. Duty to control and safety. **If body as well as item scanning then below applies:** Ethical – there is a perception that this involves the viewing of person at 'skin level', i.e. naked – although this is not the case – it does remain an issue of concern with the general public. Safeguards – controlled viewing of images, same sex viewer. EUP believe there was potential to retain images which may lead to an ethical issue, this therefore on SOP and the rationale for retention. There is an element of consent to this scanning when buying a flight ticket as the scan is a security requirement. (A refusal may lead to longer security routes / checks and possibly a body search?)
Radar – through wall	This could range from low to high depending on use	If covert use – should be subject to full consideration around justification, proportionality, necessity and authorisation.
Radar – passive tracking	In a hostage situation – low. Otherwise medium.	Limited, members of the panel understand, from the literature made available, that location/movement of individuals is assessed through data collected from various and numerous sources and that images are not likely to be detailed. Covert use, particularly as it will likely be into private premises, will require the necessary authorisation for use to determine justification, proportionality and necessity.
Radar – marine	Low	None
Radar – MIMO array	Low if used in hostage situations – rising to medium if used in pro active investigation	No significant issues as no detailed images are obtained although use into private premises may raise issue and a requirement for the appropriate authorisation.
GPS – car tracker	Low	None – owner aware, advertised by manufacturer as selling point, usually advertised on the vehicle. (Providing information is not further used/processed).
Space – spy satellites	The panel considers the level of intrusiveness could range from low to high dependent on the use of the technology and the ability of the technology with regard to the level of detail it can detect be it visual or audio.	Audio and video monitoring of another State would certainly involve some legal/ethical considerations. Monitoring of any individual and any private premises for CT or organised crime investigation/operation would also involve some issues and would require the appropriate authorisation.
UAV	Limited due to presence of technology being known to public however, level will increase if use covertly or on type of sensor.	Covert use is dependent on deployment being authorised around justification, proportionality and necessity and the type of sensor.
Sound – bug	High	There is a high level of legal and ethical issues that can be managed through authorisation of use of this equipment as being justified, proportionate and necessary together with audited use.
Sound	Low	None
Data – mobile phone tap	High	Major legal and ethical considerations – interception of communications is considered to be amongst the most intrusive forms of covert activity in many member states and any such access/use of the data by an LEA should be subject of the appropriate level of authorisation to ensure justification, proportionality and necessity, with the authorisation level usually being at the most senior level.
Data Analysis – SCIIMS	Low/medium	Potential issues but felt to be dependent on the data source that will feed into this system.
Data Analysis – Hemolia	Medium – because the effectiveness is based on the analysis of the content of personal communication and financial data.	Whilst under development access to and use of financial and communications data will potentially create issues but use by law enforcement should be authorised as being proportionate, necessary and justified.
Data Analysis – Omnifind	Medium	There would be legal and ethical considerations relating to accessing the data from other sources and how this is achieved. Any such access/use of the data by a LEA should be subject of the appropriate level of authorisation to ensure justification, proportionality and necessity.
Data Transfer Analysis – name recognition.	Low level of intrusiveness if person has knowledge. If covert use, or further process of personal information that a person was not aware was to be used for scanning, argue the level of intrusiveness increases.	Limited regarding any legal/ethical issue. However, if deployed on data set that an individual did not know was to be subject of such a scan there may be a data protection issue and infringement of privacy.
Network – AIS	Low	None – if used in process referred to – single item use
Network	Low	None
Network & Interface	Low/medium	Subject to use…as the panel understands…it will fuse incoming data from other sources which may require authorisation in their own right…Proactive use may require authorisation around proportionality and necessity, if this equipment is (capable of) being used as a stand alone piece of kit.. There is potential for consideration of significant legal requirements in case of crowd control in context to public assemblies.
Biological	Dependent on use: Overt – low Covert – medium	There would be legal and ethical considerations relating to any covert use of this equipment and any such use by a LEA should be subject of the appropriate level of authorisation to ensure justification, proportionality and necessity.
Chemical	Dependent on use: Overt – low Covert – medium	There would be legal and ethical considerations relating to any covert use of this equipment and any such use by a LEA should be subject of the appropriate level of authorisation to ensure justification, proportionality and necessity.
Radioactive	Low, however, depends if used covertly in a pro active role/investigation	Only if covert use and minimal if use is properly authorised as being justified, proportionate and necessary.
X-Ray – luggage screening	Low	No legal issues. Pre-requirement for flights and entry to buildings/locations. Duty to control and safety.
MM-Wave	Low	No legal issues. Pre-requirement for flights. Duty to control and safety. Ethical – there is a perception that this involves the viewing of person at 'skin level', i.e. naked – although this is not the case – it does remain an issue of concern with the general public. Safeguards – controlled viewing of images, same sex viewer. EUP believe there was potential to retain images which may lead to an ethical issue, this therefore on SOP and the rationale for retention. There is an element of consent to this scanning when buying a flight ticket as the scan is a security requirement. (A refusal may lead to longer security routes / checks and possibly a body search?)

Figure 2: Table of EUP normative assessments of technologies (blank text indicating no ethical risk, green a low risk, yellow medium and red high).

3. A Normative Framework for Serious Crime

DETECTER focused on counter-terrorism detection technology. The SURVEILLE project widens the focus to serious and organised crime. This is significant for the normative basis on which the use of surveillance techniques is justified. Acts of terrorism threaten life – indeed, many argue that this is their distinctive feature.[21] Even uses of the ethically riskiest surveillance technologies are justifiable in the case of threats to life. However, the category of serious crime includes a variety of threats that fall short of this – robberies, organised football violence and fraud, for example, may all count in certain circumstances as serious organised crime, without always endangering life. Under what circumstances would ethically risky surveillance techniques be justified here?

The first point to be noted is that in certain cases, even 'low level' crime can have high impacts. Most burglary, for example, would not reach the threshold for the use of very intrusive methods. But very frequent operations in a single area by an organized gang of burglars might justify unusually intrusive detection measures. The same might be true of criminal behaviour that seemed to target the extremely vulnerable, or that was directed again and again at particular people or families or groups, such that the lives of those people were made miserable. In the ordinary, non-legal sense of 'proportionate', it might be proportionate to direct unusually intrusive police resources or efforts against the perpetrators of such crimes, even though none of the victims were in danger of being killed. There are at least five factors which may lead to more intrusive methods being appropriate. These are significant financial loss; use of violence; threat to public order; organisation; and significant financial gain. Each of these five possible features of crime can elevate it to a level where intrusion and other risks would be appropriate. In section 4, I elaborate further on how the badness of each of these features relates to the

[21] See for example the DETECTER Deliverable 6.1 for an argument that the category of terrorism should be reserved for life threatening attacks www.detecter.bham.ac.uk/D6.1LegalAnalysisCritiqueDoctrines.doc.

normative basis for ethically risky methods, but first I explain how this framework expands on the normative framework of DETECTER.

The proposed SURVEILLE framework retains the categorization of ethical risks of surveillance technology developed in DETECTER. Where it differs is in widening out the normative grounds that justify the taking of these ethical risks. To be sure, threats to life, social order and infrastructure occur in crimes other than terrorism, justifying risky methods. However, 'violence' is a more relevant category to serious crime in general than life threatening violence. This is because the majority of the violence that would merit risky surveillance does not in fact threaten life. Threats to infrastructure, while an important category when considering terrorism, can fall under the category of threats to social order, or significant financial loss when considering serious crime. Terrorism, while important, represents a small subset of the crimes that could merit risky methods, as illustrated in Figure 3.

	Sample Crimes	**Possible Disutilities of Crime**	**Possible Law Enforcement Technologies**
Serious Financial Loss	Burglary	Financial difficulty	CCTV,
	Identity Theft	Financial difficulty	Computer monitoring malware
Violence	Armed Burglary	Injury, fear	CCTV
	Racketeering	Fear, loss, threat to person	CCTV, placement of miniaturised microphones (bugging) in premises where extortion or planning takes place.
	Bombing of civilian area	Death, serious injury	Wire taps
Public Order	Sabotage of power station	Threat to public infrastructure	Wire taps
	Looting	Panic, violence, fear	CCTV
Organisation	Racketeering	Expansion of	Placement of

		criminal enterprise	miniaturised microphones (bugging) in premises where extortion or planning takes place.
	Money laundering	Expansion of criminal enterprise	Data mining
Serious Financial Gain	Drug trafficking	Expansion of criminal enterprise, social impact of drug trade	placement of miniaturised microphones (bugging) in premises where planning takes place, wire taps
	Identity theft	Expansion of criminal enterprise, financial loss	Computer monitoring malware

Figure 3: Table of moral risks of sample crimes, some associated disutilities and possible law enforcement technologies, showing highlighted category of terrorism as a subset.

The disutilities listed in Figure 3 are not all equal in normative importance. To underline this a hierarchy of disutilities is presented in Figure 4. This is not intended as definitive – such a hierarchy can only be partial. Instead it is intended to show that while threats to welfare associated with serious crime vary considerably in their severity, matters much less severe than the disutilities associated with terrorism are still normatively significant, as elaborated upon in section 4.

Disutilities arising from serious crime	**Comment**
Death	Life is the condition of a life plan and any human welfare.
Serious Injury	Directly threatening to welfare and potentially greatly constraining of life plans and future welfare.
Threat to Public Infrastructure	Transport, electricity, running water are all very important to life plans and are part of human welfare.
Expansion of criminal enterprise	Organised criminal enterprises likely to represent threats to welfare by virtue of the full range of activity it takes part in,

	and expansion may represent further threats either by leading to more of the same kind of activity (e.g. shipping more cocaine) or by diversifying (e.g. credit card fraudsters moving on to engaging in online drug dealing).
Social impact of drug trade	Various disutilities involved in drug addiction for individuals taking them, but also must consider the violence and criminality often associated both with the trade at street level and of users to pay for their habit.
Financial difficulty	May undermine range of life plans which are important to welfare.
Fear	Bad in itself because of its subjective unpleasantness, and may also be bad because people may needlessly avoid areas where they fear further crime, thus constraining their lives.
Panic	Bad in itself because of its subjective unpleasantness, and may be disruptive of life plans contributing to welfare.

Figure 4. Possible hierarchy of disutitlities generated by serious crimes.

4. Normatively Grounding the Framework

Section 3 introduced significant financial loss, use of violence, threat to public order, organisation and significant financial gain as features of serious crime that may elevate specific instances of it to a level where intrusion and other risks would be appropriate. In what follows, the normative significance of each of these factors is outlined to justify the use of riskier investigative methods.

i. Significant Financial Loss

Crime, especially property crime, frequently entails financial loss. Not all financial loss reaches a level at which it seriously affects the victim's welfare, but it is clear enough that financial loss *can* have such an impact – financial loss can deprive people of their principal means of satisfying many important means and goals, and can also lead to future difficulty, for example by resulting in businesses failing or problems with personal debt. What counts as 'significant financial loss' has to be considered relative to the victim, rather than in absolute terms. For example, the

theft of £100 from a millionaire will have a much smaller impact than the theft of £100 from someone in poverty.[22]

Furthermore, low level crimes perpetrated on individuals can result in significant loss given sustained repetition. Where we begin to talk not about an isolated burglary but a sustained campaign repeatedly targeting the same area, we quite plausibly may talk of financial loss with a significant detrimental effect on welfare.

The individual cannot reasonably expect the state to repel all threats to their welfare – that would place far too onerous requirements on the state. However, where significant threats to welfare exist and those threats are easily preventable, the individual has some basis for expecting preventive measures. For example, if publicly provided housing is badly designed in ways that make burglary easy, the individual has a reason to expect the relevant housing authority to introduce protective measures equipment for those affected, perhaps including the use of more intrusive technology.

Significant financial loss does not only result from theft. Vandalism could inflict significant financial loss, for example, by making a place of business unusable, or damaging equipment vital to the running of a business. Pertinently, damage to various kinds of infrastructure threatened by terrorism, and by cyber terrorism, would also be capable of inflicting massive financial damage on businesses. Furthermore, fraud can also be a source of significant financial loss – consider the impact of the discovery in early 2013 that meat sold in the UK and Ireland as beef was adulterated with horsemeat and with pork.[23] As well as financial loss resulting from withdrawn and destroyed stock,[24] businesses have had contracts terminated and retailers may suffer financial loss due to loss of trust.

[22] Assuming other things being equal – e.g. that physical violence or the threat or violence has not been used.

[23] See, for example; http://www.bbc.co.uk/news/uk-21375594

[24] See, for example; http://www.guardian.co.uk/world/2013/feb/08/how-horsemeat-scandal-unfolded-timeline

ii. Use of Violence

The state claims a special right to use force not generally available to citizens. While there remains a presumption against the use of force even by the police, and the use of force has to be justified, it is something the police have much greater entitlement to than the general public – if an ordinary member of the public uses force by and large the sole rationale they can cite is self-defence. One corollary of this is a special responsibility to protect people from violence. One form this protection may take is investigation, including ethically risky investigation. Threats to life fall under the category of violence, but violence does not have to threaten life to affect welfare. Injuries and physical harm threaten welfare, but violence does not even have to harm to affect welfare significantly. There are at least three reasons for this.

Firstly there are many more disutilities of violence than the direct causing of death or injury – psychological disutilities, like trauma and fear – and further disutilities may arise if people change their behaviour as a result of violence, avoiding public places because they feel less safe. Violence, particularly persistent violence, can have its own 'chilling effect'. Many of these disutilities are shared by threats of violence. By definition threats of violence do not inflict physical harm, but threats of violence can inflict trauma and fear all the same. When criminal organisations run protection rackets, the fact they do so with the threat of violence is significant whether or not anyone is actually attacked as a result. These are therefore cases that could be appropriately investigated with ethically riskier methods.

Secondly, even what one might call 'low level' violence, which didn't cause significant physical harm, could acquire significance incrementally, as it surely does in campaigns of physical harassment. This is because even low level violence can make a person's life a misery when part of a pattern that combines to undermine a person's sense of safety in everyday life. Furthermore, the combination of significant financial loss and violence can be an additional exacerbating factor in

assessing the severity of persistent low level crime. If part of a pattern, a physical attack that does not cause significant harm can lead someone plausibly to fear more significant physical harm the next time around.

Finally, violent attacks which do not cause significant physical harm may also be more significant when directed against vulnerable people, like children, the frail or the disabled. This includes threats of violence, to which vulnerable groups are especially vulnerable because of their evidence powerlessness.

iii. Threat to Public Order

Public order can be undermined by violence, but it can also be undermined by activity short of violence, including threats of violence. Damage to infrastructure, or transport, even where it does not directly put people in danger, can lead to the uncertainty and panic where people lose their confidence in public order – for example a shut down of public transport in a large city would not have to involve direct threats to personal safety to have this effect. The recent EU VITA project provides a taxonomy of threats to critical infrastructure which is relevant here.[25] (This taxonomy is also used in the EU FOCUS project as the basis for identifying exogenous threats).[26]

However, the state's duty to protect against threats to public order can be in tension with other state duties, like protection of free speech and free assembly. This arises, for example, in the case of certain demonstrations offensive to other sectors of the community, likely to result in civil disorder. The state has a duty to protect both the rights of free speech and the right of the public to safety.

[25] See http://vita.iabg.eu/

[26] See, for example: FOCUS Deliverable D5.1 chapter 8 http://www.focusproject.eu/web/focus/home

There are a number of recent cases where disorder has broken out on the streets, seemingly with the assistance of online social networking technologies. Should communications over such media be viewed on a par with telephone taps, as the most severe kind of intrusion? When is it appropriate for policing authorities to view these kinds of messages? In what follows I consider these questions in relation to the UK riots of 2011[27], the Northern Irish flags protest of 2012-13[28] and the arrest of far right English Defence League members in a Whitehall pub.[29]

In the summer of 2011 riots broke out in London originally in protest over the shooting of Mark Duggan by the Metropolitan Police, but soon escalating into mass looting and vandalism. Police were criticised for not intervening 'robustly' enough with criminality.[30] Whether or not the criticism was fair, it is certainly true that there was a sound normative basis for tackling such criminality robustly. This point was usually made in relation to the use of force, but the same considerations weigh on the use of intrusive methods. Much of this criminality seemed to be coordinated with the use of social networking technology, specifically Blackberry Messenger, with some commentators labelling the whole episode "The Blackberry Riots".[31] This led some to call for interception of such messages (or indeed to shut the service down), in the face of objections to a supposed intrusion.[32] Would interception of Blackberry Messenger messages be unacceptably intrusive in this case? No. 'Fishing expeditions', where messages were intercepted speculatively, could not be justified, as indeed they cannot even in the most serious cases of threat to life, but given a

[27] For an overview of news sources see: http://en.wikipedia.org/wiki/2011_England_riots.

[28] For an overview of news sources see: http://en.wikipedia.org/wiki/Belfast_City_Hall_flag_protests.

[29] See, for example: http://www.guardian.co.uk/uk/2011/nov/11/edl-arrests-london-occupy-armistice-day.

[30] See, for example: http://www.telegraph.co.uk/news/uknews/crime/8690819/London-riots-David-Cameron-says-police-must-be-more-robust.html

[31] See, for example: http://www.economist.com/node/21525976.

[32] See, for example: http://www.guardian.co.uk/uk/2011/aug/08/london-riots-blackberry-messenger-looting.

good reason to suspect that a specific person was sending out messages coordinating looting and violence likely to be a danger to public order (say on the basis of verified reports that the person had sent out a number of such messages already), monitoring their further messages would seem proportionate.

In Northern Ireland, navigating a path between threats to public safety and rights to free assembly and political and religious demonstration is particularly fraught. Starting on the 3rd of December 2012, demonstrations over a contentious Council decision limiting the flying of the Union flag gave rise to a sustained campaign of protests. These inflicted heavy financial losses on local businesses over the Christmas period and continued to do so until the end of January 2013. Again, at one stage the Police Service of Northern Ireland were criticised for being too light-touch in their intervention.[33] Freedom of public assembly and protest are of the utmost importance in a democratic society. However, it is possible to do justice to this principle while granting the justifiability of more active intervention. For one thing, the right to protest is not the right to indefinite protest. One of the exacerbating factors in people's assessment of the legitimacy of the protesters actions was the fact that the protests had by that point been continuing for months.[34] By this point the public were inclined to think, even when sympathetic to the grievance, that they had had their say. It may well have also been influenced by the fact that the protests had also disrupted the local economy considerably, with claims of up to 300 jobs lost in a week.[35] (This is not to deny the difficulty of maintaining the balance – elsewhere in Northern Ireland police were also heavily

[33] See for example this typical Belfast Telegraph opinion piece: http://www.belfasttelegraph.co.uk/opinion/columnists/lindy-mcdowell/isnt-it-about-time-psni-got-tough-on-uvf-godfathers-29039616.html and this report of police defense of their response: http://www.u.tv/news/PSNI-defend-actions-over-city-rioting/207cd605-3f85-4140-9fd0-4ea61bd9463a.

[34] See the relevant survey results at: http://www.bbc.co.uk/news/uk-northern-ireland-21331212 and analysis in the spotlight programme itself http://www.bbc.co.uk/programmes/b01qlfbk.

[35] See, for example: http://www.bbc.co.uk/news/uk-northern-ireland-21052749.

criticised for heavy-handed policing of flags protests.[36]) The flags protests provide another case of social networking as a tool of organisation – for example a Facebook group announcing and disseminating information on the so-called 'operation standstill' – a plan to bring Belfast city centre businesses to a halt by a series of protests blocking roads into and out of the city.[37]

The possibility of sparking disorder is a threat in European jurisdictions in general, particularly in relation to policing demonstrations by fringe political groups advocating racist policies. Liberal respect for the right to demonstrate conflicts in a number of ways with the state's commitment to upholding public order, most starkly in the case of governments outlawing protests by extremist groups altogether.[38] More relevant to the current discussion is the monitoring of such groups. To take one example, nearly 180 members of the far right English Defence League (EDL) were arrested in a pub in 2011 following monitoring of exchanges on a Facebook page where the gathering was arranged and also apparently stating a plan to attack members of the left wing 'Occupy Movement'.[39] Was this monitoring unacceptable? Again no. This case is even more clear cut in terms of intrusiveness than the London riots Blackberry Messenger case, as the messages were posted on an open page where anyone could theoretically join and see them if they looked. Monitoring fora like this is more like surveillance of public space. That is not to say that there are no norms constraining watching – after all, this is not true of actual surveillance of public spaces. But it is to say that the evidential threshold for policing authorities to look at such spaces is lower than in the case of person to person communications such as Blackberry Messenger.

---

[36] See, for example: http://www.ballyclaregazette.co.uk/articles/news/31788/flag-protesters-psni-were-heavy-handed/ and http://www.bbc.co.uk/news/uk-northern-ireland-foyle-west-21157482.

[37] See, for example: http://www.newsletter.co.uk/news/operation-standstill-v-operation-sitin-1-4675400 and http://www.newsletter.co.uk/news/operation-standstill-v-operation-sitin-1-4675400

[38] See for example the banning of a series of planned London marches of the EDL: http://www.bbc.co.uk/news/uk-england-london-20084304.

[39] See these screenshots of the Facebook page in question:http://blog.fredrikwalloe.com/2011/11/edl-group-threatens-occupy-lsx.html

Where both privacy and the principle of free speech provide a weak basis for police surveillance and deployment in these cases, proportionality (in its ordinary sense) may provide a better one. The seriousness of plans to commit violence need to be weighed in the light of the fact that much that is said in online fora is never followed up on – lies and exaggerations are common, and many armchair radicals are never going to represent a genuine physical threat to anyone. This is certainly true in the case of the EDL, studies on which seem to indicate that the overwhelming majority of its online membership confine their involvement to online activity alone and would never take the step of attending a real world event.[40] It seems doubtful whether an exchange between online activists expressing an intention to commit violence ought to be treated as a genuine threat in all cases. All that needs to be established here is that people communicating in online public fora planning violence do not themselves have a claim that they are illegitimately intruded upon when police monitor such communications, nor do they have cause for complaint where police err on the side of caution. The question of proportionality turns on a satisfactory quantification of how plausible a given threat is.

More controversial have been cases where police pursued intrusive methods against apparently peaceful groups, such as environmental activists. At the most controversial end of the scale was the placement of an undercover officer inside an environmental organisation.[41] Automatic Number Plate Recognition systems have also been used to track non-violent environmental activists, in some cases amounting to harassment.[42] These examples are troubling from the perspective of liberal theory, because the commitment to freedom of thought and association does not seem to them to be outweighed by a genuine threat of violence or to public

[40] See the Demos (2011) report: *Inside the EDL: populist politics in a digital age*.

[41] See, for example: http://www.guardian.co.uk/uk/2011/jan/09/undercover-office-green-activists

[42] See, for example: http://www.guardian.co.uk/uk/2009/oct/25/surveillance-police-number-plate-recognition

order.[43] While the undercover police incident has been acknowledged to be a mistake,[44] police defend the close, sometimes intrusive, scrutiny of environmental organisations on the grounds of the threat of sabotage to infrastructure and the threat to public order this may pose. As we have seen, this is a supportable line of argument – there can be cases when this would justify severe intrusion. However, once again, quantifying the nature of the threat is necessary to assess the proportionality of risky methods with satisfaction.

iv. Organisation

The significance of organised as opposed to non-organised crime lies in the difference in kind of the threat organised groups may pose to the public. Organised criminal enterprises, needless to say, span an enormous range in terms of size, complexity and threat. But not only the largest and most threatening are legitimate targets of ethically risky surveillance. A gang of car thieves can be a legitimate object of intrusive scrutiny, for example, even though the theft of a car by an individual could not justify such methods alone, because an organisation of thieves can be much more dangerous.[45]

Larger and more sophisticated criminal organisations are rightly regarded as one of the most significant policing threats in Europe.[46] They also pose risks to the public in strikingly diverse ways. For example criminal organisation may also take the form of persons involved in crime acquiring non-criminal businesses. While these can of

[43] See, for example: UN Rapporteur Maina Kiai's description of the affair as 'unacceptable in a democracy' http://www.guardian.co.uk/uk/2013/jan/23/un-official-undercover-police-scandal

[44] See, for example: http://www.guardian.co.uk/environment/2012/feb/02/how-mark-kennedy-went-rogue

[45] We can also note that the significance of organisation adds to the proportionality of monitoring social networking communications for criminal activity in the cases discussed under the heading of threats to public order in part *iii*.

[46] See for example the statements of the EU Internal Security Strategy: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/internal-security/internal-security-strategy/index_en.htm.

course form a non-criminal revenue stream, they can also be useful for explicitly criminal purposes. For example they may provide a channel for money laundering, or they may also provide useful fronts, to innocently explain regular presence and activity of the members of an organisation at a particular location.

In some member state jurisdictions criminal organisations reach such a level of complexity and sophistication that they are able to compete for and indeed win government construction contracts. This can raise still further grounds for ethically risky investigative techniques, as the dangers from reckless practices aimed at undercutting rival bidders to the disregard of building regulations can pose a severe threat to public safety. Such illegal construction projects also frequently make use of coerced labour in violation of fundamental rights.[47] These practices, where they occur, add to the urgency of preventing criminal groups from continuing their practices and thus the proportionality of intrusive methods. Note that this is a separate basis from that of the violence such groups often employ as well. A group of organised individuals carrying out construction contracts by using reckless illegal methods could become a legitimate object of intrusive surveillance because of the threat to the public such an organisation poses.

Larger criminal networks may also operate across borders. Effective responses to transnational crime will frequently require police cooperation and intelligence-sharing across borders. However, this has its own ethical risks as well. For one thing, the DETECTER normative framework suggests that sharing information acquired intrusively with a wider audience itself counts as a further intrusion. Even more seriously, the spread of intelligence may multiply risks of error. Stripped of its original context, and details such as the strength of an assessment that someone is, for example, 'a suspected associate' of a criminal group, makes it harder to assess the appropriateness of further action. When information is shared with another country's policing authorities, control over how that intelligence is going to be used

[47] See the International Labour Organization report 'Forced Labour: an EU Problem': http://www.ilo.org/global/about-the-ilo/newsroom/news/WCMS_184972/lang--en/index.htm

is lost. Intelligence sharing with regimes that are not human rights respecting is the starkest example of ethical danger this poses.

v. Significant Financial Gain

The clearest criterion of success for a criminal enterprise is financial gain for the perpetrators. The state has an obligation to combat criminal organisations and it makes sense to prioritise the successful ones. Transnational criminal organisations are particularly relevant here.[48] Particular crimes, and certain established supply routes,[49] may therefore merit ethically risky surveillance for reasons distinct and additional to any use of violence and other direct threats to human welfare. Investigating crime which is involved with these highly profitable sectors of organised crime therefore has a stronger normative basis.

Conclusion

The identified features of crime are defensible reasons for policing authorities to use ethically risky technologies, and provides a framework that extends beyond DETECTER's focus on counter-terrorism. As in the case of counter-terrorism, the state's obligation to protect its citizens from violence and direct threats to personal safety plays a key role, but the framework recognises other significant reasons in addition: loss to the victim, organisation on the part of the perpetrators and profitability of the criminal enterprise. Financial loss, while not as significant as direct threats to the person, can nevertheless significantly damage welfare. And while it may make no difference to the individual whether her house was burgled by a single burglar or an organised gang of burglars, but this does make a difference to

[48] For example (*Wired*, February 2011) gives a figure of $128 billion as a total estimated value for global criminal activity based on UNODC figures http://www.wired.com/magazine/2011/01/ff_orgchart_crime/

[49] See UNODC 2010 report 'The Globalisation of Crime: a Transnational Organised Crime Threat Assessment' for one account of globally significant supply chains http://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf

the danger the perpetrator poses to the public. Likewise when her car is stolen by a gang of car thieves, the victim may not care how much money the gang is making from this, but it may well be relevant to how high a priority the gang is to policing authorities. Safeguarding the the welfare of the citizen is not just a matter of protecting her from violence.

Bibliography

Bartlett, Jamie and Mark Littler. 2011. *Inside the EDL*. London: Demos.

Branting, L. Karl. 2005, 'Name Matching in Law Enforcement and Counter-Terrorism' *ICAIL Workshop on Data Mining, Information Extraction, and Evidentiary Reasoning for Law Enforcement and Counter-Terrorism* Bologna, Italy.

DeCew, Judith. 1997. *In Pursuit of Privacy*. New York: Cornell University Press

English, Richard. 2009. *Terrorism: How to Respond*. Oxford: Oxford University Press

Hillyard, Paddy. 1993. *Suspect Community*. Pluto Press

Moeckli, Daniel. 2008. *Human Rights and Non-Discrimination in the 'War on Terror'*. Oxford: Oxford University Press

Pantazis, Christina and Simon Pemberton. 'From the Old to the New Suspect Community' in The British Journal of Criminology. 2009 vol. 49 p 646-66

Rawls, John. 1971. *A Theory of Justice*. Cambridge MA: Harvard University Press

Roberts, Adam. 1989. 'Ethics, Terrorism and Counter-Terrorism' in Terrorism and Political Violence. Vol. 1. no. 1

Spalek, Basia, El Alwa and Laura McDonald. 2008. *Police-Muslim Engagement and Partnerships for the Purpose of Counter-Terrorism: an Examination*. University of Birmingham

Steinberg, Jonny. 2009. *Thin Blue*. Johnny Ball with Open Society Foundation for South Africa.

Tavani, Herman. 'KDD, data mining, and the challenge for normative privacy' in Ethics and Information Technology. 1999. vol. 1. no. 4 p. 265.

Annex 1: Technology information sheets completed by the End User Panel

SURVEILLE PROJECT END USER PANEL – INPUT	
NAME OF EUP MEMBER: Full Panel	
Description of Equipment – Biological – Airborne IMS Bio Product Mass Spectro For Detecting ions	
What category of serious crime does the technology impact on?	CT and potentially serious and organised crimes involving product contamination / extortion or similar.
Comment regarding claim as to use by developer.	For use in the rapid detection of biological agents and early detection of attacks, together with assistance in the recovery plan post any attack. The panel understands that this equipment remains under development and dependant on the sensitivity of the equipment, may also be appropriate for use in prevention and proactive work, either in an overt or covert arena.
Is the technology capable of use in LEA work regarding prevention, intelligence, proactive / reactive detection – (or both).	The overt use of this equipment – post incident and therefore in a reactive situation would be an expectation of the public. As detailed above, this equipment could also be used in an overt preventative and pro-active arena if capable of scanning individuals and items of property for such pathogens. This equipment could also be used in a covert / proactive manner if capable of conducting such scans without the knowledge of the individual.
Is the technology capable of use in Overt / covert investigation or both?	Both – subject to comments above.
Assess effectiveness i.e. Significant / of benefit / minimal / unknown / indeterminable (Go to Website / back to Delft for details if necessary)	Significant.
Any significant Legal / ethical issues?	There would be legal and ethical considerations relating to any covert use of this equipment and any such use by a LEA should be subject of the appropriate level of authorisation to

	ensure justification, proportionality and necessity.
View regarding Level of intrusiveness – high, medium, low, cannot determine.	Dependant on use: Overt – low Covert – medium.
Cost Effective	Significant – specifically in relation to early detection of attack and detection of any pathogens when there is a claim of contamination of goods / extortion. If established as being sensitive enough, could also be of benefit regarding detection of any traces on individuals potentially planning such attacks.
Any other comments?	

SURVEILLE PROJECT **END USER PANEL – INPUT**	
NAME OF EUP MEMBER: Full Panel	
Description of Equipment – CCTV and Activity Detection - IPS Activity Detection	
What category of serious crime does the technology impact on?	CT and all categories of serious and organised crime, together will all levels of other crime.
Comment regarding claim as to use by developer.	The significant positive benefits of the use of CCTV equipment in law enforcement work is well established and proven. With this equipment, the panel understands that an additional functionality to the basic CCTV function is the ability to detect either motion on screens or unusual motion outside of what can be normally expected for the area/s that is covered / under surveillance.
Is the technology capable of use in LEA work regarding prevention, intelligence, proactive / reactive detection – (or both).	The overt use of CCTV is recognised as a significant tool in crime prevention and reassurance to the public / communities. CCTV is appropriate for use in all stages of intelligence and investigation activity, both at the reactive and proactive stages.
Is the technology capable of use in Overt / covert investigation or both?	Both.

Assess effectiveness i.e. Significant / of benefit / minimal / unknown / indeterminable (Go to Website / back to Delft for details if necessary)	Significant.
Any significant Legal / ethical issues?	Overt positioning of CCTV equipment by public bodies, and in private and commercial locations is widespread. This is regularly advertised and within the knowledge of individuals and the public at large. Covert use of CCTV poses a different aspect and falls into two broad categories: Deployment and use of equipment by a law enforcement agency as part of their activities relating to intelligence, proactive or reactive investigative responsibilities or, Covert use of overtly placed CCTV equipment by LEAs for the proactive surveillance of individuals. There will also be legal and ethical considerations relating to use of overt or covert CCTV equipment that is used to monitor activity in private premises. In reactive investigation (post incident) the use of CCTV from all overt sources should pose little or no legal / ethical issues subject to a LEA's seizure and retention procedures being appropriate. The specific deployment of CCTV equipment for a covert use by a LEA, together with the targeted (and thereby covert) use of overt systems by a LEA should be subject of the appropriate level of authorisation to ensure justification, proportionality and necessity.
View regarding Level of intrusiveness – high, medium, low, cannot determine.	Dependant on use: Overt – low Covert – medium to high depending on where deployed.
Cost Effective	Significant – specifically in relation to the added advantage of the ability to alert users to either any motion / activity and / or the ability to alert users to unusual activity (eg out of place / location).
Any other comments?	

SURVEILLE PROJECT END USER PANEL – INPUT	
NAME OF EUP MEMBER: Full Panel	
Description of Equipment – CCTV and Infra Red – Near Field	
What category of serious crime does the technology impact on?	CT and all categories of serious and organised crime, together will all levels of other crime.
Comment regarding claim as to use by developer.	The significant positive benefits of the use of CCTV equipment in law enforcement work is well established and proven. With this equipment, the panel understands that an additional functionality to the basic CCTV operation is the ability to monitor / detect / record activity during the hours of darkness or when there is limited light available due to the infra red capability.
Is the technology capable of use in LEA work regarding prevention, intelligence, proactive / reactive detection – (or both).	The overt use of CCTV is recognised as a significant tool in crime prevention and reassurance to the public / communities. CCTV is appropriate for use in all stages of intelligence and investigation activity, both at the reactive and proactive stages.
Is the technology capable of use in Overt / covert investigation or both?	Both.
Assess effectiveness i.e. Significant / of benefit / minimal / unknown / indeterminable (Go to Website / back to Delft for details if necessary)	Significant.
Any significant Legal / ethical issues?	Overt positioning of CCTV equipment by public bodies, and in private and commercial locations is widespread. This is regularly advertised and within the knowledge of individuals and the public at large. Covert use of CCTV poses a different aspect and falls into two broad categories: Deployment and use of equipment by a law enforcement

	agency as part of their activities relating to intelligence, proactive or reactive investigative responsibilities or, Covert use of overtly placed CCTV equipment by LEAs for the proactive surveillance of individuals. There will also be legal and ethical considerations relating to use of overt or covert CCTV equipment that is used to monitor activity in private premises. In reactive investigation (post incident) the use of CCTV from all overt sources should pose little or no legal / ethical issues subject to a LEA's seizure and retention procedures being appropriate. The specific deployment of CCTV equipment for a covert use by a LEA, together with the targeted (and thereby covert) use of overt systems by a LEA should be subject of the appropriate level of authorisation to ensure justification, proportionality and necessity.
View regarding Level of intrusiveness – high, medium, low, cannot determine.	Dependant on use: Overt – low Covert – medium to high depending on where deployed.
Cost Effective	Significant – specifically in relation to the added advantage of the ability to use this equipment during the hours of darkness, when there is limited light available (through infra red capability) and more detailed product through (near field) coverage.
Any other comments?	

SURVEILLE PROJECT END USER PANEL – INPUT	
NAME OF EUP MEMBER: Full Panel	
Description of Equipment – CCTV and Infra Red – Wide Area	
What category of serious crime does the technology impact on?	CT and all categories of serious and organised crime, together will all levels of other crime.

Comment regarding claim as to use by developer.	The significant positive benefits of the use of CCTV equipment in law enforcement work is well established and proven. With this equipment, the panel understands that an additional functionality to the basic CCTV operation is the ability to monitor / detect / record activity during the hours of darkness or when there is limited light available due to the infra red capability.
Is the technology capable of use in LEA work regarding prevention, intelligence, proactive / reactive detection – (or both).	The overt use of CCTV is recognised as a significant tool in crime prevention and reassurance to the public / communities. CCTV is appropriate for use in all stages of intelligence and investigation activity, both at the reactive and proactive stages.
Is the technology capable of use in Overt / covert investigation or both?	Both.
Assess effectiveness i.e. Significant / of benefit / minimal / unknown / indeterminable (Go to Website / back to Delft for details if necessary)	Significant.
Any significant Legal / ethical issues?	Overt positioning of CCTV equipment by public bodies, and in private and commercial locations is widespread. This is regularly advertised and within the knowledge of individuals and the public at large. Covert use of CCTV poses a different aspect and falls into two broad categories: Deployment and use of equipment by a law enforcement agency as part of their activities relating to intelligence, proactive or reactive investigative responsibilities or, Covert use of overtly placed CCTV equipment by LEAs for the proactive surveillance of individuals. There will also be legal and ethical considerations relating to use of overt or covert CCTV equipment that is used to monitor activity in private premises. In reactive investigation (post incident) the use of CCTV from all overt sources should pose little or no legal / ethical issues

	subject to a LEA's seizure and retention procedures being appropriate. The specific deployment of CCTV equipment for a covert use by a LEA, together with the targeted (and thereby covert) use of overt systems by a LEA should be subject of the appropriate level of authorisation to ensure justification, proportionality and necessity.
View regarding Level of intrusiveness – high, medium, low, cannot determine.	Dependant on use: Overt – low Covert – medium to high depending on where deployed.
Cost Effective	Significant – specifically in relation to the added advantage of the ability to use this equipment during the hours of darkness, when there is limited light available (through infra red capability) and through greater distance (wild field) coverage.
Any other comments?	

SURVEILLE PROJECT END USER PANEL – INPUT	
NAME OF EUP MEMBER: Full Panel	
Description of Equipment – CCTV visual semi automated camera Guppy	
What category of serious crime does the technology impact on?	CT and all categories of serious and organised crime, together will all levels of other crime.
Comment regarding claim as to use by developer.	The significant positive benefits of the use of CCTV equipment in law enforcement work is well established and proven. For this equipment, the availability of the automatic trigger obviously has benefits with regard to prolonging use (power / battery supply).
Is the technology capable of use in LEA work regarding prevention, intelligence, proactive / reactive	The overt use of CCTV is recognised as a significant tool in crime prevention and reassurance to the public / communities.

detection – (or both).	Appropriate for use in all stages of intelligence and investigation activity, both at the reactive and proactive stages.
Is the technology capable of use in Overt / covert investigation or both?	Both.
Assess effectiveness i.e. Significant / of benefit / minimal / unknown / indeterminable (Go to Website / back to Delft for details if necessary)	Significant.
Any significant Legal / ethical issues?	Overt positioning of CCTV equipment by public bodies, and in private and commercial locations is widespread. This is regularly advertised and within the knowledge of individuals and the public at large. Covert use of CCTV poses a different aspect and falls into two broad categories: Deployment and use of equipment by a law enforcement agency as part of their activities relating to intelligence, proactive or reactive investigative responsibilities or, Covert use of overtly placed CCTV equipment by LEAs for the proactive surveillance of individuals. There will also be legal and ethical considerations relating to use of overt or covert CCTV equipment that is used to monitor activity in private premises. In reactive investigation (post incident) the use of CCTV from all overt sources should pose little or no legal / ethical issues subject to a LEA's seizure and retention procedures being appropriate. The specific deployment of CCTV equipment for a covert use by a LEA, together with the targeted (and thereby covert) use of overt systems by a LEA should be subject of the appropriate level of authorisation to ensure justification, proportionality and necessity.
View regarding Level of intrusiveness – high, medium, low, cannot determine.	Dependant on use: Overt – low Covert – medium to high depending on where deployed.

Cost Effective	Significant – and in relation to the added advantage of the automatic trigger used with this specific equipment, further cost benefit in view savings relating to power source and potential for no requirement for physical operation.
Any other comments?	

SURVEILLE PROJECT END USER PANEL – INPUT	
NAME OF EUP MEMBER: Full Panel	
Description of Equipment – CCTV – Visual Spectrum Dome - Zoom, Tilt and Rotate	
What category of serious crime does the technology impact on?	CT and all categories of serious and organised crime, together will all levels of other crime.
Comment regarding claim as to use by developer.	The significant positive benefits of the use of CCTV equipment in law enforcement work is well established and proven. With this equipment, there is the added benefit through being networked and the panel understands that an additional functionality to the basic CCTV function is the ability for operators to manage the product through the availability to zoom in / out and change the direction of the camera – i.e. through not being fixed.
Is the technology capable of use in LEA work regarding prevention, intelligence, proactive / reactive detection – (or both).	The overt use of CCTV is recognised as a significant tool in crime prevention and reassurance to the public / communities. CCTV is appropriate for use in all stages of intelligence and investigation activity, both at the reactive and proactive stages.
Is the technology capable of use in Overt / covert investigation or both?	Both.
Assess effectiveness i.e. Significant /	Significant.

of benefit / minimal / unknown / indeterminable (Go to Website / back to Delft for details if necessary)	
Any significant Legal / ethical issues?	Overt positioning of CCTV equipment by public bodies, and in private and commercial locations is widespread. This is regularly advertised and within the knowledge of individuals and the public at large. Covert use of CCTV poses a different aspect and falls into two broad categories: Deployment and use of equipment by a law enforcement agency as part of their activities relating to intelligence, proactive or reactive investigative responsibilities or, Covert use of overtly placed CCTV equipment by LEAs for the proactive surveillance of individuals. There will also be legal and ethical considerations relating to use of overt or covert CCTV equipment that is used to monitor activity in private premises. In reactive investigation (post incident) the use of CCTV from all overt sources should pose little or no legal / ethical issues subject to a LEA's seizure and retention procedures being appropriate. The specific deployment of CCTV equipment for a covert use by a LEA, together with the targeted (and thereby covert) use of overt systems by a LEA should be subject of the appropriate level of authorisation to ensure justification, proportionality and necessity.
View regarding Level of intrusiveness – high, medium, low, cannot determine.	Dependant on use: Overt – low Covert – medium to high depending on where deployed.
Cost Effective	Significant – specifically in relation to the added advantage of the ability for operators to manage the product of this equipment through it not being fixed.
Any other comments?	

SURVEILLE PROJECT END USER PANEL – INPUT	
NAME OF EUP MEMBER: Full Panel	
Description of Equipment – CCTV visual spectrum (dome fixed)	
What category of serious crime does the technology impact on?	CT and all categories of serious and organised crime, together will all levels of other crime.
Comment regarding claim as to use by developer.	The significant positive benefits of the use of CCTV equipment in law enforcement work is well established and proven. With this equipment, the ability to cover larger and distant areas will have additional benefits, together with the capacity to be networked.
Is the technology capable of use in LEA work regarding prevention, intelligence, proactive / reactive detection – (or both).	The overt use of CCTV is recognised as a significant tool in crime prevention and reassurance to the public / communities. CCTV is appropriate for use in all stages of intelligence and investigation activity, both at the reactive and proactive stages.
Is the technology capable of use in Overt / covert investigation or both?	Both.
Assess effectiveness i.e. Significant / of benefit / minimal / unknown / indeterminable (Go to Website / back to Delft for details if necessary)	Significant.
Any significant Legal / ethical issues?	Overt positioning of CCTV equipment by public bodies, and in private and commercial locations is widespread. This is regularly advertised and within the knowledge of individuals and the public at large. Covert use of CCTV poses a different aspect and falls into two broad categories: Deployment and use of equipment by a law enforcement agency as part of their activities relating to intelligence, proactive or reactive investigative responsibilities or,

	Covert use of overtly placed CCTV equipment by LEAs for the proactive surveillance of individuals. There will also be legal and ethical considerations relating to use of overt or covert CCTV equipment that is used to monitor activity in private premises. In reactive investigation (post incident) the use of CCTV from all overt sources should pose little or no legal / ethical issues subject to a LEA's seizure and retention procedures being appropriate. The specific deployment of CCTV equipment for a covert use by a LEA, together with the targeted (and thereby covert) use of overt systems by a LEA should be subject of the appropriate level of authorisation to ensure justification, proportionality and necessity.
View regarding Level of intrusiveness – high, medium, low, cannot determine.	Dependant on use: Overt – low Covert – medium to high depending on where deployed.
Cost Effective	Significant – specifically in relation to the added advantage of the ability to be used in larger areas, for greater distances and trough being networked.
Any other comments?	

SURVEILLE PROJECT END USER PANEL – INPUT	
NAME OF EUP MEMBER: Full Panel	
Description of Equipment – CCTV – Visual Spectrum - Fixed	
What category of serious crime does the technology impact on?	CT and all categories of serious and organised crime, together will all levels of other crime.
Comment regarding claim as to use by developer.	The significant positive benefits of the use of CCTV equipment in law enforcement work is well established and proven.

	This equipment provides basic CCTV monitoring functionality.
Is the technology capable of use in LEA work regarding prevention, intelligence, proactive / reactive detection – (or both).	The overt use of CCTV is recognised as a significant tool in crime prevention and reassurance to the public / communities. CCTV is appropriate for use in all stages of intelligence and investigation activity, both at the reactive and proactive stages.
Is the technology capable of use in Overt / covert investigation or both?	Both.
Assess effectiveness i.e. Significant / of benefit / minimal / unknown / indeterminable (Go to Website / back to Delft for details if necessary)	Significant but potentially less benefit when compared to moveable cameras owing to its fixed position.
Any significant Legal / ethical issues?	Overt positioning of CCTV equipment by public bodies, and in private and commercial locations is widespread. This is regularly advertised and within the knowledge of individuals and the public at large. Covert use of CCTV poses a different aspect and falls into two broad categories: Deployment and use of equipment by a law enforcement agency as part of their activities relating to intelligence, proactive or reactive investigative responsibilities or, Covert use of overtly placed CCTV equipment by LEAs for the proactive surveillance of individuals. There will also be legal and ethical considerations relating to use of overt or covert CCTV equipment that is used to monitor activity in private premises. In reactive investigation (post incident) the use of CCTV from all overt sources should pose little or no legal / ethical issues subject to a LEA's seizure and retention procedures being appropriate. The specific deployment of CCTV equipment for a covert use by a LEA, together with the targeted (and thereby covert) use of overt systems by a LEA should be subject of the

	appropriate level of authorisation to ensure justification, proportionality and necessity.
View regarding Level of intrusiveness – high, medium, low, cannot determine.	Dependant on use: Overt – low Covert – medium to high depending on where deployed.
Cost Effective	Significant.
Any other comments?	

SURVEILLE PROJECT END USER PANEL – INPUT	
NAME OF EUP MEMBER: Full Panel	
Description of Equipment – Chemical – Detection by Antibody (SALIENT)	
What category of serious crime does the technology impact on?	CT and Serious and Organised Crime – particularly offences involving drugs, firearms and extortion.
Comment regarding claim as to use by developer.	A hand held device to rapidly anylise and detect traces of explosives, toxicology and chemicals.
Is the technology capable of use in LEA work regarding prevention, intelligence, proactive / reactive detection – (or both).	The overt use of this equipment – post incident and therefore in a reactive situation would be an expectation of the public and could be used to manage public safety and prevention of spread. This equipment could also be used in a covert / proactive manner if capable of conducting such scans without the knowledge of the individual.
Is the technology capable of use in Overt / covert investigation or both?	Both – subject to comments above.
Assess effectiveness i.e. Significant /	Significant.

of benefit / minimal / unknown / indeterminable (Go to Website / back to Delft for details if necessary)	
Any significant Legal / ethical issues?	There would be legal and ethical considerations relating to any covert use of this equipment and any such use by a LEA should be subject of the appropriate level of authorisation to ensure justification, proportionality and necessity.
View regarding Level of intrusiveness – high, medium, low, cannot determine.	Dependant on use: Overt – low Covert – medium.
Cost Effective	Significant – specifically in relation to early detection of incident / attack and in preventing any spread.
Any other comments?	

SURVEILLE PROJECT END USER PANEL – INPUT	
NAME OF EUP MEMBER: Full Panel	
Description of Equipment – Chemical – Explosive Detection Near Harbour (UNCOS)	
What category of serious crime does the technology impact on?	CT
Comment regarding claim as to use by developer.	Equipment used to detect neutrons and therefore IEDs and explosives, specifically in harbours.
Is the technology capable of use in LEA work regarding prevention, intelligence, proactive / reactive detection – (or both).	The overt use of this equipment – prior to any incident is to prevent any possibility of an attack in a harbour environment. This equipment could be used in a covert / proactive manner if capable of conducting such scans without the knowledge of owners / users of vessels.

Is the technology capable of use in Overt / covert investigation or both?	Both – subject to comments above.
Assess effectiveness i.e. Significant / of benefit / minimal / unknown / indeterminable (Go to Website / back to Delft for details if necessary)	Significant.
Any significant Legal / ethical issues?	There would be legal and ethical considerations relating to any covert use of this equipment and any such use by a LEA should be subject of the appropriate level of authorisation to ensure justification, proportionality and necessity.
View regarding Level of intrusiveness – high, medium, low, cannot determine.	Dependant on use: Overt – low Covert – medium.
Cost Effective	Significant – specifically in relation to preventing any attack.
Any other comments?	

SURVEILLE PROJECT END USER PANEL – INPUT	
NAME OF EUP MEMBER: Full Panel	
Description of Equipment – Chemical – Gas Chromatography Drugs Detector (DIRAC)	
What category of serious crime does the technology impact on?	Serious and Organised Crime – Drug offences at all levels.
Comment regarding claim as to use by developer.	Handheld device - equipment used to detect drugs, pre-cursor chemicals and agents giving rapid results. There would need to be a proven record of use that eliminates any possibility of false reading or contamination due to sensitivity of the equipment.

Is the technology capable of use in LEA work regarding prevention, intelligence, proactive / reactive detection – (or both).	The overt use of this equipment – as a pre-condition of entry at a border, or on any form of travel can be seen as a preventative measure or - as a reactive stage of an investigation or operation if drugs are detected and found. This equipment could be used in a covert / proactive manner if capable of conducting such scans without the knowledge of individuals.
Is the technology capable of use in Overt / covert investigation or both?	Both – subject to comments above.
Assess effectiveness i.e. Significant / of benefit / minimal / unknown / indeterminable (Go to Website / back to Delft for details if necessary)	Significant.
Any significant Legal / ethical issues?	There would be legal and ethical considerations relating to any covert use of this equipment and any such use by a LEA should be subject of the appropriate level of authorisation to ensure justification, proportionality and necessity.
View regarding Level of intrusiveness – high, medium, low, cannot determine.	Dependant on use: Overt – low Covert – medium.
Cost Effective	Significant.
Any other comments?	

SURVEILLE PROJECT END USER PANEL – INPUT	
NAME OF EUP MEMBER: Full Panel	
Description of Equipment – Chemical – Novel Detection Technique (COMMONSENSE)	
What category of serious crime does the technology impact on?	CT and feasibly serious and organised crime in relation to drug manufacturing.

Comment regarding claim as to use by developer.	The technology is specifically designed to detect explosives (and feasibly drug chemicals and precursor agents?) in water – thereby allowing for detection in water outlets of properties.
Is the technology capable of use in LEA work regarding prevention, intelligence, proactive / reactive detection – (or both).	This equipment is most likely to be used in a covert / proactive manner to detect ongoing unlawful activity in the manufacturing of a device or drug compounds. Could be used in an overt / reactive manner post incident – such as to test when there has been a terrorist attack on water supplies or to assess safety of water supply after an industrial accident?
Is the technology capable of use in Overt / covert investigation or both?	Both – subject to comments above.
Assess effectiveness i.e. Significant / of benefit / minimal / unknown / indeterminable (Go to Website / back to Delft for details if necessary)	Significant but does depend on ability to detect traces of chemicals / compounds and how results are interpreted in evidence / court.
Any significant Legal / ethical issues?	Covert use of this equipment may involve legal and ethical considerations depending on where any secret monitoring of wastewater from a property is being monitored and any such use by a LEA should be subject of the appropriate level of authorisation to ensure justification, proportionality and necessity.
View regarding Level of intrusiveness – high, medium, low, cannot determine.	Dependant on use: Overt – low Covert – medium.
Cost Effective	Significant – specifically in relation to early detection of incident / attack and in preventing any spread.
Any other comments?	

SURVEILLE PROJECT
END USER PANEL – INPUT

NAME OF EUP MEMBER: Full Panel	
Description of Equipment – Chemical – Precursor and Drug Detection (CUSTOM)	
What category of serious crime does the technology impact on?	Serious and organised crime in relation to drug manufacture, supply and importation.
Comment regarding claim as to use by developer.	The project aims to assess viability of using two techniques to detect trace elements of drugs - LASER Photo Acoustic Spectroscopy and the UV induced Fluorescence. The panel understand that it is primarily designed for use at borders, airports, harbours and at custom check points.
Is the technology capable of use in LEA work regarding prevention, intelligence, proactive / reactive detection – (or both).	The overt use of this equipment – as a pre-condition of entry at a border or on any form of travel can be seen as a preventative measure or as a reactive stage of an investigation or operation if drugs are detected and found. This equipment is suitable for use in a covert / proactive manner if capable of conducting such scans without the knowledge of individuals.
Is the technology capable of use in Overt / covert investigation or both?	Both – subject to comments above.
Assess effectiveness i.e. Significant / of benefit / minimal / unknown / indeterminable (Go to Website / back to Delft for details if necessary)	Significant - especially due to the claim that the equipment will have an ability to detect traces of chemicals / compounds without false readings.
Any significant Legal / ethical issues?	There would be legal and ethical considerations relating to any covert use of this equipment and any such use by a LEA should be subject of the appropriate level of authorisation to ensure justification, proportionality and necessity.
View regarding Level of intrusiveness – high, medium, low, cannot determine.	Dependant on use: Overt – low Covert – medium.
Cost Effective	Significant.

Any other comments?	

SURVEILLE PROJECT END USER PANEL – INPUT	
NAME OF EUP MEMBER: Full Panel	
Description of Equipment – Chemical – Standoff Optical Detector of Explosives (OPTIX)	
What category of serious crime does the technology impact on?	CT
Comment regarding claim as to use by developer.	A device designed to detect explosives from a distance of approximately 20 metres.
Is the technology capable of use in LEA work regarding prevention, intelligence, proactive / reactive detection – (or both).	Overt use of this equipment is feasible in dealing with a threatened attack – in order to assess the specific location of a device. It would also be suitable for overt use post incident in order to try and detect / locate any booby trap devices. This equipment could also be used in a covert / proactive manner if capable of conducting such scans without the knowledge of the individual (e.g. when intelligence has suggested a device is being made or has been planted, or in the event of a suicide bomber). Consideration would be needed around the safety offered to an operative when using the equipment – 20m would be dependant on the size of the device.
Is the technology capable of use in Overt / covert investigation or both?	Both – subject to comments above.
Assess effectiveness i.e. Significant / of benefit / minimal / unknown / indeterminable (Go to Website / back to Delft for details if necessary)	Significant.

Any significant Legal / ethical issues?	There would be legal and ethical considerations relating to any covert use of this equipment and any such use by a LEA should be subject of the appropriate level of authorisation to ensure justification, proportionality and necessity.
View regarding Level of intrusiveness – high, medium, low, cannot determine.	Dependant on use: Overt – low Covert – medium.
Cost Effective	Significant – specifically in relation to early detection of incident / attack.
Any other comments?	

SURVEILLE PROJECT END USER PANEL – INPUT	
NAME OF EUP MEMBER: Full Panel	
Description of Equipment – DATA ANALYSIS – detection of money laundering HEMOLIA	
What category of serious crime does the technology impact on?	Serious organised crime (predominantly money laundering) and CT
Comment regarding claim as to use by developer.	Project in development, there are no publications or media releases available.
Is the technology capable of use in LEA work regarding prevention, intelligence, proactive / reactive detection – (or both).	Intelligence, reactive and pro active.
Is the technology capable of use in Overt / covert investigation or both?	Both
Assess effectiveness i.e. Significant / of benefit / minimal / unknown /	If developed in line with website claims – potentially significant.

indeterminable (Go to Website / back to Delft for details if necessary)	
Any significant Legal / ethical issues?	Whilst under development access to and use of financial and communications data will potentially create issues but use by law enforcement should be authorised as being proportionate, necessary and justified.
View regarding Level of intrusiveness – high, medium, low, cannot determine.	Medium - because the effectiveness is based on the analysis of the content of (personal) communication and financial data
Cost Effective	If successful in detecting money laundering on a large scale this equipment has the potential to be significantly cost effective.
Any other comments?	Project still under development – planned end date 30 April 2014

SURVEILLE PROJECT END USER PANEL – INPUT	
NAME OF EUP MEMBER: Full Panel	
Description of Equipment – DATA ANALYSIS – networked data analysis SCIIMS	
What category of serious crime does the technology impact on?	Serious organised crime (predominantly human trafficking) but also CT.
Comment regarding claim as to use by developer.	This technology is under development and subject of an EU project.
Is the technology capable of use in LEA work regarding prevention, intelligence, proactive / reactive detection – (or both).	Both

Is the technology capable of use in Overt / covert investigation or both?	Both
Assess effectiveness i.e. Significant / of benefit / minimal / unknown / indeterminable (Go to Website / back to Delft for details if necessary)	Of Benefit
Any significant Legal / ethical issues?	Potential issues but felt to be dependent on the data source that will feed into this system
View regarding Level of intrusiveness – high, medium, low, cannot determine.	Loe / medium
Cost Effective	Indeterminable
Any other comments?	This technology is under development and subject of an EU project. Whilst it would appear that it can rely on open data already in possession of law enforcement agencies, a lot depends on what other sources will be used to feed into this system and whether those sources are appropriately authorised.

SURVEILLE PROJECT END USER PANEL – INPUT	
NAME OF EUP MEMBER: Full Panel	
Description of Equipment – Data – Analysis (OMNIFIND)	
What category of serious crime does the technology impact on?	CT and serious & organised crime.
Comment regarding claim as to use by developer.	An IT programme to manage data fusion and information from different sources.
Is the technology capable of use in LEA work regarding prevention, intelligence, proactive / reactive	The panel understand that this equipment / programme will search for and detect similarities (or recurring omissions etc)

detection – (or both).	in data from various sources. This equipment is suitable for use in a covert / proactive manner and in the main for intelligence purposes.
Is the technology capable of use in Overt / covert investigation or both?	Covert.
Assess effectiveness i.e. Significant / of benefit / minimal / unknown / indeterminable (Go to Website / back to Delft for details if necessary)	Significant.
Any significant Legal / ethical issues?	There would be legal and ethical considerations relating to accessing the data from other sources and how this is achieved. Any such access / use of the data by a LEA should be subject of the appropriate level of authorisation to ensure justification, proportionality and necessity.
View regarding Level of intrusiveness – high, medium, low, cannot determine.	Medium.
Cost Effective	Indeterminable.
Any other comments?	

SURVEILLE PROJECT END USER PANEL – INPUT	
NAME OF EUP MEMBER: Full Panel	
Description of Equipment – Data – Mobile Phone Tap (PTS)	
What category of serious crime does the technology impact on?	CT and serious & organised crime.
Comment regarding claim as to use by developer.	IT software that allows for the recording and monitoring of use of mobile telephones including calls, texts, photos and

	videos, together with the location of the mobile.
Is the technology capable of use in LEA work regarding prevention, intelligence, proactive / reactive detection – (or both).	This technology requires the software to be actually applied to the mobile handset subject of the intended surveillance and the panel understand that it has primarily been developed - and is advertised for use, by private individuals (e.g. for tracking cheating partners etc) as opposed to public bodies and therefore LEAs. However, whilst the lawful interception of communications by LEAs is managed through completely different processes and technology, use of such devices in law enforcement work remains feasible and would serve to assist at all stages of an investigation.
Is the technology capable of use in Overt / covert investigation or both?	Covert.
Assess effectiveness i.e. Significant / of benefit / minimal / unknown / indeterminable (Go to Website / back to Delft for details if necessary)	Significant.
Any significant Legal / ethical issues?	Major legal and ethical considerations – interception of communications is considered to be amongst the most intrusive forms of covert activity in many member states and any such access / use of the data by a LEA should be subject of the appropriate level of authorisation to ensure justification, proportionality and necessity, with the authorisation level usually being at the most senior level.
View regarding Level of intrusiveness – high, medium, low, cannot determine.	High
Cost Effective	Significant.
Any other comments?	

SURVEILLE PROJECT END USER PANEL – INPUT	
NAME OF EUP MEMBER: Full Panel	
Description of Equipment: DATA TRANSFER ANALYSIS – name recognition	
What category of serious crime does the technology impact on?	Both Serious Crime and CT
Comment regarding claim as to use by developer.	Regularly used with such information as e-Borders and Advanced Passenger Information on flights (API).
Is the technology capable of use in LEA work regarding prevention, intelligence, proactive / reactive detection – (or both).	Both – for tracking
Is the technology capable of use in Overt / covert investigation or both?	Both overt and covert
Assess effectiveness i.e. Significant / of benefit / minimal / unknown / indeterminable (Go to Website / back to Delft for details if necessary)	Significant benefit - tracking of individuals wanted for commission of offence/s or covert tracking of suspect
Any significant Legal / ethical issues?	Limited regarding any legal / ethical issue. However, if deployed on data set that an individual did not know was to be subject of such a scan there maybe a data protection issue and infringement of privacy.
View regarding Level of intrusiveness – high, medium, low, cannot determine.	Low level of intrusiveness if person has knowledge. If covert use, or further process of personal information that an individual was not aware was to be used for scanning, argue the level of intrusiveness increases.
Cost Effective	Low cost – high value
Any other comments?	

SURVEILLE PROJECT END USER PANEL – INPUT	
NAME OF EUP MEMBER: Full Panel	
Description of Equipment – DNA – rapid DNA analysis MiDAS	
What category of serious crime does the technology impact on?	Not applicable – see comments below.
Comment regarding claim as to use by developer.	Not applicable – see comments below.
Is the technology capable of use in LEA work regarding prevention, intelligence, proactive / reactive detection – (or both).	Not applicable – see comments below.
Is the technology capable of use in Overt / covert investigation or both?	Not applicable – see comments below.
Assess effectiveness i.e. Significant / of benefit / minimal / unknown / indeterminable (Go to Website / back to Delft for details if necessary)	Not applicable – see comments below.
Any significant Legal / ethical issues?	Not applicable – see comments below.
View regarding Level of intrusiveness – high, medium, low, cannot determine.	Not applicable – see comments below.
Cost Effective	Not applicable – see comments below.
Any other comments?	The EUP have only viewed that as a reactive investigation tool to

	provide rapid results at crime scenes. **E-mail from EUP Member 14 January 2013** With respect to my action on the worksheet you can see that the product (MiDAS) has not made it to market. This is primarily because of the closure of the Forensic Science Service who were the lead organisation in the development. http://cordis.europa.eu/fetch?CALLER=RESULINK_EN&ACTION=D&RCN=53394

SURVEILLE PROJECT **END USER PANEL – INPUT**	
NAME OF EUP MEMBER: Full Panel	
Description of Equipment: **GPS – car tracker SN**	
What category of serious crime does the technology impact on?	Vehicle theft – potentially high value
Comment regarding claim as to use by developer.	Proven technology
Is the technology capable of use in LEA work regarding prevention, intelligence, proactive / reactive detection – (or both).	Reactive / detection – post theft of vehicle. Prevention – manufacturers fitting of the device is advertised.
Is the technology capable of use in Overt / covert investigation or both?	Overt- is used with knowledge of owner
Assess effectiveness i.e. Significant / of benefit / minimal / unknown / indeterminable (Go to Website / back to Delft for details if necessary)	Significant benefit – leads to property recovery and apprehension of offenders.
Any significant Legal / ethical issues?	None – owner aware, advertised by manufacturer as selling point, usually advertised on the vehicle. (Providing information is not further used / processed).

View regarding Level of intrusiveness – high, medium, low, cannot determine.	Low
Cost Effective	High value - vehicle or equipment recovery
Any other comments?	The EUP only approach this on the basis of a manufacturer fit to the vehicle or equipment, use of the data to locate such property and no further process of the technology product.

SURVEILLE PROJECT END USER PANEL – INPUT	
NAME OF EUP MEMBER: Full Panel	
Description of Equipment – IMAGE PROCESSING – crowd and riot	
What category of serious crime does the technology impact on?	Crime (predominantly large scale public disorder)
Comment regarding claim as to use by developer.	EUP understand that this technology involves the development of image processing that then gives an alert at certain behaviour patterns.
Is the technology capable of use in LEA work regarding prevention, intelligence, proactive / reactive detection – (or both).	Both
Is the technology capable of use in Overt / covert investigation or both?	Both
Assess effectiveness i.e. Significant / of benefit / minimal / unknown / indeterminable (Go to Website / back to Delft for details if necessary)	Of benefit

Any significant Legal / ethical issues?	If the software conducts analysis of crowds and not individuals, from the information available it would appear that there are no major legal or ethical issues.
View regarding Level of intrusiveness – high, medium, low, cannot determine.	Low
Cost Effective	Cannot be determined
Any other comments?	

SURVEILLE PROJECT END USER PANEL – INPUT	
NAME OF EUP MEMBER: Full Panel	
Description of Equipment – IMAGE PROCESSING – people counting and density	
What category of serious crime does the technology impact on?	Crime (predominantly large scale public disorder)
Comment regarding claim as to use by developer.	Crowd control in mass events e.g. public concerts, early detection of critical mass effects and the onset of panic
Is the technology capable of use in LEA work regarding prevention, intelligence, proactive / reactive detection – (or both).	Both
Is the technology capable of use in Overt / covert investigation or both?	Both
Assess effectiveness i.e. Significant / of benefit / minimal / unknown / indeterminable (Go to Website / back to Delft for details if necessary)	Of benefit
Any significant Legal / ethical issues?	If the software conducts analysis of crowds and not

	individuals, from the information available it would appear that there are no major legal or ethical issues. However, in some EU member states there maybe potential for legal issues in case of use in context of monitoring public assembly (Germany)
View regarding Level of intrusiveness – high, medium, low, cannot determine.	Low
Cost Effective	Cannot be determined
Any other comments?	
SURVEILLE PROJECT **END USER PANEL – INPUT**	
NAME OF EUP MEMBER: Full Panel	
Description of Equipment – INFRA RED – motion detector	
What category of serious crime does the technology impact on?	All categories of crime and CT – if premises are protected for such purposes
Comment regarding claim as to use by developer.	Proven
Is the technology capable of use in LEA work regarding prevention, intelligence, proactive / reactive detection – (or both).	Prevention / pro active investigation
Is the technology capable of use in Overt / covert investigation or both?	Both – depending on where placed / advertised
Assess effectiveness i.e. Significant / of benefit / minimal / unknown / indeterminable (Go to Website / back to Delft for details if necessary)	Significant benefit

Any significant Legal / ethical issues?	None – if used in process referred to - single item use
View regarding Level of intrusiveness – high, medium, low, cannot determine.	Low
Cost Effective	High
Any other comments?	

SURVEILLE PROJECT END USER PANEL – INPUT	
NAME OF EUP MEMBER: Full Panel	
Description of Equipment: MM-WAVE – whole body scanner EQO	
What category of serious crime does the technology impact on?	All serious and organised crime and CT involving weapons
Comment regarding claim as to use by developer.	Proven technology
Is the technology capable of use in LEA work regarding prevention, intelligence, proactive / reactive detection – (or both).	Prevention, intelligence and pro active investigation
Is the technology capable of use in Overt / covert investigation or both?	Overt only
Assess effectiveness i.e. Significant / of benefit / minimal / unknown / indeterminable (Go to Website / back to Delft for details if necessary)	Significantly effective

Any significant Legal / ethical issues?	No legal issues. Pre requirement for flights. Duty to control and safety. Ethical – there is a perception that this involves the viewing of person at 'skin level', i.e. naked – although this is not the case – it does remain an issue of concern with the general public. Safeguards – controlled viewing of images, same sex viewer. EUP believe there was potential to retain images which may lead to an ethical issue, this therefore on SOP and the rationale for retention. There is an element of consent to this scanning when buying a flight ticket as the scan is a security requirement. (A refusal may lead to longer security routes / checks and possibly a body search?)
View regarding Level of intrusiveness – high, medium, low, cannot determine.	Low
Cost Effective	This is an alternative to other security systems and processes. However, the EUP believe it requires a minimum of 3 persons to operate and cost effectiveness may therefore be limited, however, when balanced against the preventative potential (detection of weapons and explosives) is considered to be of significant value.
Any other comments?	

SURVEILLE PROJECT **END USER PANEL – INPUT**	
NAME OF EUP MEMBER: Full Panel	
Description of Equipment: **NETWORK – AIS ship location detection and identification**	
What category of serious crime does the technology impact on?	The tracking of ships in investigations relating to Serious Crime and Counter-terrorism

Comment regarding claim as to use by developer.	Proven
Is the technology capable of use in LEA work regarding prevention, intelligence, proactive / reactive detection – (or both).	Can be used in both elements of investigation (reactive and proactive).
Is the technology capable of use in Overt / covert investigation or both?	Both. This equipment is openly available and its product is open source material. Covert use would involve proactive monitoring.
Assess effectiveness i.e. Significant / of benefit / minimal / unknown / indeterminable (Go to Website / back to Delft for details if necessary)	Limited benefit – other sources available and general knowledge of equipment.
Any significant Legal / ethical issues?	None
View regarding Level of intrusiveness – high, medium, low, cannot determine.	Low
Cost Effective	Limited cost and high return
Any other comments?	EUP based assessment on knowledge of this equipment being a requirement for all passenger carrying vessels and commercial ships. Obvious any use by an LEA for live or historic tracking of ships would use open source material but that pro active tracking of a vessel would become covert activity. **Note** – EUP aware that this device could be used in search and rescue and is also capable of being switched off

SURVEILLE PROJECT END USER PANEL – INPUT	
NAME OF EUP MEMBER: Full Panel	
Description of Equipment – NETWORK – SIRIUS 3RK3	
What category of serious crime does the technology impact on?	All categories of crime and CT – if premises protected for such purposes
Comment regarding claim as to use by developer.	Proven
Is the technology capable of use in LEA work regarding prevention, intelligence, proactive / reactive detection – (or both).	Prevention / pro active
Is the technology capable of use in Overt / covert investigation or both?	Both – depending on where placed / advertised
Assess effectiveness i.e. Significant / of benefit / minimal / unknown / indeterminable (Go to Website / back to Delft for details if necessary)	Significant benefit
Any significant Legal / ethical issues?	None – if used in process referred to - single item use
View regarding Level of intrusiveness – high, medium, low, cannot determine.	Low
Cost Effective	High
Any other comments?	Added benefits regarding smoke / heat / fire. Also, detection of bodily movement when deployed in the home of elderly or vulnerable people therefore overt for health and wellbeing. No issues providing no further process of data.

SURVEILLE PROJECT END USER PANEL – INPUT	
NAME OF EUP MEMBER: Full Panel	
Description of Equipment – NETWORK – UGM 2040	
What category of serious crime does the technology impact on?	All categories of crime and CT – if premises protected for such purposes
Comment regarding claim as to use by developer.	Proven
Is the technology capable of use in LEA work regarding prevention, intelligence, proactive / reactive detection – (or both).	Prevention / pro active
Is the technology capable of use in Overt / covert investigation or both?	Both – depending on where placed / advertised
Assess effectiveness i.e. Significant / of benefit / minimal / unknown / indeterminable (Go to Website / back to Delft for details if necessary)	Significant benefit
Any significant Legal / ethical issues?	None – if used in process referred to - single item use
View regarding Level of intrusiveness – high, medium, low, cannot determine.	Low
Cost Effective	High
Any other comments?	Added benefits regarding smoke / heat / fire. Also, detection of bodily movement when deployed in the home of elderly or vulnerable people therefore overt for health and wellbeing. No issues providing no further process of data.

SURVEILLE PROJECT END USER PANEL – INPUT	
NAME OF EUP MEMBER: Full Panel	
Description of Equipment: NETWORK & INTERFACE – AMFIS data fusion for ground control	
What category of serious crime does the technology impact on?	CT, Organised Crime and Public Disorder
Comment regarding claim as to use by developer.	To analyse various sources of data (sensor technique as well as optical information) and predict dangers, to detect hidden persons, to classify peculiar behaviour or carryout intelligent surveillance of spaces and rooms.
Is the technology capable of use in LEA work regarding prevention, intelligence, proactive / reactive detection – (or both).	Prevention, intelligence and pro active together with reactive capability if data is capable of being recorded.
Is the technology capable of use in Overt / covert investigation or both?	Both
Assess effectiveness i.e. Significant / of benefit / minimal / unknown / indeterminable (Go to Website / back to Delft for details if necessary)	Of benefit
Any significant Legal / ethical issues?	Subject to use (see any other comments below). Pro active use may require authorisation around proportionality and necessity, if this equipment is (capable of) being used as a 'stand alone' piece of kit. There is potential for consideration of significant legal requirements in case of crowd control in context to public assemblies.
View regarding Level of intrusiveness – high, medium, low, cannot determine.	Low / medium
Cost Effective	Cannot determine

Any other comments?	As the panel understands the use of this equipment, it will fuse incoming data from other sources which may require authorisation in their own right.

SURVEILLE PROJECT END USER PANEL – INPUT	
NAME OF EUP MEMBER: Full Panel	
Description of Equipment – RADAR – acoustic sensor network	
What category of serious crime does the technology impact on?	Organised crime (potentially in the main fire arm related) and CT
Comment regarding claim as to use by developer.	This technology is still under research. The equipment is being tested to determine classification of targets (sounds) in built up /urban locations. Examples of what the equipment can determine between includes by way of example – gunfire vehicle engines and walking (human pedestrians)
Is the technology capable of use in LEA work regarding prevention, intelligence, proactive / reactive detection – (or both).	Both
Is the technology capable of use in Overt / covert investigation or both?	Both but the panel considers that covert use will be more common
Assess effectiveness i.e. Significant / of benefit / minimal / unknown / indeterminable (Go to Website / back to Delft for details if necessary)	Of benefit
Any significant Legal / ethical issues?	Minimal if the equipment is used to alert / locate gunfire and differentiate between other sounds (vehicular). With regard to locating people no major issues if detecting trespassers. However, covertly locating individuals would increase the legal and ethical issues and would require the appropriate authorisation.
View regarding Level of intrusiveness	Low / medium

– high, medium, low, cannot determine.	
Cost Effective	Indeterminable
Any other comments?	

SURVEILLE PROJECT END USER PANEL – INPUT	
NAME OF EUP MEMBER: Full Panel	
Description of Equipment: RADAR – array-based concealed weapon detection rad	
What category of serious crime does the technology impact on?	All serious and organised crime and CT involving weapons
Comment regarding claim as to use by developer.	Further information is required regarding whether this relates to body image and or item image
Is the technology capable of use in LEA work regarding prevention, intelligence, proactive / reactive detection – (or both).	Prevention, intelligence and pro active investigation
Is the technology capable of use in Overt / covert investigation or both?	Both overt and covert
Assess effectiveness i.e. Significant / of benefit / minimal / unknown / indeterminable (Go to Website / back to Delft for details if necessary)	Significantly effective
Any significant Legal / ethical issues?	No legal issues. Pre requirement for flights. Duty to control and safety. **If body as well as item scanning then below applies:** Ethical – there is a perception that this involves the viewing of person at 'skin level', i.e. naked – although this is not the case

	– it does remain an issue of concern with the general public. Safeguards – controlled views of images, same sex viewer. EUP believe there was potential to retain images which may lead to an ethical issue, this therefore on SOP and the rationale for retention. There is an element of consent to this scanning when buying a flight ticket as the scan is a security requirement. (A refusal may lead to longer security routes / checks and possibly a body search?)
View regarding Level of intrusiveness – high, medium, low, cannot determine.	Low
Cost Effective	This is an alternative to other security systems and processes. However, the EUP believe it requires a minimum of 3 persons to operate and cost effectiveness may therefore be limited, however, when balanced against the preventative potential (detection of weapons and explosives) is considered to be of significant value.
Any other comments?	

SURVEILLE PROJECT END USER PANEL – INPUT	
NAME OF EUP MEMBER: Full Panel	
Description of Equipment – RADAR – array based through wall radar	
What category of serious crime does the technology impact on?	CT and all crime
Comment regarding claim as to use by developer.	Agree – subject to Operator training and environmental factors and variables.
Is the technology capable of use in	Both

LEA work regarding prevention, intelligence, proactive / reactive detection – (or both).	
Is the technology capable of use in Overt / covert investigation or both?	Both
Assess effectiveness i.e. Significant / of benefit / minimal / unknown / indeterminable (Go to Website / back to Delft for details if necessary)	EUP believe this an emerging piece of technological equipment that is under development and may require further evaluation.
Any significant Legal / ethical issues?	If covert use – should be subject to full consideration around justification, proportionality, necessity and authorisation.
View regarding Level of intrusiveness – high, medium, low, cannot determine.	This could range between low to high depending on use
Cost Effective	Dependent on use – impacts on cost effectiveness
Any other comments?	The EUP believe that this equipment is openly used in fire / rescue type situations. However, the panel have approached their assessment from a covert use / tactic.

SURVEILLE PROJECT END USER PANEL – INPUT	
NAME OF EUP MEMBER: Full Panel	
Description of Equipment: RADAR – Marine Radar	
What category of serious crime does the technology impact on?	The tracking of ships in investigations relating to Serious Crime and Counter-terrorism
Comment regarding claim as to use by developer.	Proven

Is the technology capable of use in LEA work regarding prevention, intelligence, proactive / reactive detection – (or both).	Can be used in both elements of investigation (reactive and proactive).
Is the technology capable of use in Overt / covert investigation or both?	Both, however, whilst this equipment is openly available users require a licence to possess and use and its product is not open source material. Covert use would involve proactive monitoring.
Assess effectiveness i.e. Significant / of benefit / minimal / unknown / indeterminable (Go to Website / back to Delft for details if necessary)	Of benefit – other sources available and general knowledge of equipment.
Any significant Legal / ethical issues?	None
View regarding Level of intrusiveness – high, medium, low, cannot determine.	Low
Cost Effective	Limited cost and high return
Any other comments?	Obvious any use by an LEA for live or historic tracking of ships but that pro active tracking of a vessel would become covert activity.

SURVEILLE PROJECT END USER PANEL – INPUT	
NAME OF EUP MEMBER: Full Panel	
Description of Equipment – RADAR – MIMO array	
What category of serious crime does the technology impact on?	Organised crime and CT

Comment regarding claim as to use by developer.	In normal circumstances is issued to police forces when dealing with serious crime, when a protection / rescue scenario around victims is involved.
Is the technology capable of use in LEA work regarding prevention, intelligence, proactive / reactive detection – (or both).	Both pro active and reactive
Is the technology capable of use in Overt / covert investigation or both?	Both although panel consider covert use more common
Assess effectiveness i.e. Significant / of benefit / minimal / unknown / indeterminable (Go to Website / back to Delft for details if necessary)	Significant
Any significant Legal / ethical issues?	No significant issues as no detailed images are obtained although use into private premises may raise an issue and a requirement for the appropriate authorisation
View regarding Level of intrusiveness – high, medium, low, cannot determine.	Low if used in hostage type situations – rising to medium if used in pro active investigation
Cost Effective	Unknown
Any other comments?	

SURVEILLE PROJECT END USER PANEL – INPUT	
NAME OF EUP MEMBER: Full Panel	
Description of Equipment – RADAR – passive through wall human tracking	
What category of serious crime does	Organised crime and CT

the technology impact on?	
Comment regarding claim as to use by developer.	Still under early research stage and relevant papers and internet items are as recent as 2012
Is the technology capable of use in LEA work regarding prevention, intelligence, proactive / reactive detection – (or both).	Both pro active and reactive
Is the technology capable of use in Overt / covert investigation or both?	Capable of both, but consider that covert solutions will be the most common usage of equipment
Assess effectiveness i.e. Significant / of benefit / minimal / unknown / indeterminable (Go to Website / back to Delft for details if necessary)	Significant and of benefit (particularly with regard to hostage situations and potentially the location / movement of suspects).
Any significant Legal / ethical issues?	Limited, members of the panel understand, from the literature made available, that location / movement of individuals is assessed through data collected from various and numerous sources and that images are not likely to be detailed. Covert use, particularly as it will likely be into private premises, will require the necessary authorisation for use to determine justification, proportionality and necessity.
View regarding Level of intrusiveness – high, medium, low, cannot determine.	In a hostage situation – low. Otherwise medium
Cost Effective	Unknown at this stage
Any other comments?	

SURVEILLE PROJECT END USER PANEL – INPUT	
NAME OF EUP MEMBER: Full Panel	
Description of Equipment – RADAR – short range for intrusion detection	
What category of serious crime does the technology impact on?	All categories of crime and CT – if premises are protected for such purposes
Comment regarding claim as to use by developer.	Proven
Is the technology capable of use in LEA work regarding prevention, intelligence, proactive / reactive detection – (or both).	Prevention / pro active investigation
Is the technology capable of use in Overt / covert investigation or both?	Both – depending on where placed / advertised
Assess effectiveness i.e. Significant / of benefit / minimal / unknown / indeterminable (Go to Website / back to Delft for details if necessary)	Significant benefit
Any significant Legal / ethical issues?	None – if used in process referred to - single item use
View regarding Level of intrusiveness – high, medium, low, cannot determine.	Low
Cost Effective	High
Any other comments?	

SURVEILLE PROJECT END USER PANEL – INPUT	
NAME OF EUP MEMBER: Full Panel	
Description of Equipment – RADIOACTIVE – compton detector COCAE	
What category of serious crime does the technology impact on?	CT investigation and illegal nuclear / radio active waste disposal
Comment regarding claim as to use by developer.	**Assessment of equipment being undertaken by EUP Member**
Is the technology capable of use in LEA work regarding prevention, intelligence, proactive / reactive detection – (or both).	Both
Is the technology capable of use in Overt / covert investigation or both?	Both
Assess effectiveness i.e. Significant / of benefit / minimal / unknown / indeterminable (Go to Website / back to Delft for details if necessary)	Significant
Any significant Legal / ethical issues?	Only if covert use and minimal if use is properly authorised as being justified, proportionate and necessary.
View regarding Level of intrusiveness – high, medium, low, cannot determine.	Low, however, depends if used covertly in a pro active role / investigation
Cost Effective	Of benefit
Any other comments?	

SURVEILLE PROJECT END USER PANEL – INPUT	
NAME OF EUP MEMBER: Full Panel	
Description of Equipment – SOUND – ECM8000 microphone	
What category of serious crime does the technology impact on?	Serious crime and CT
Comment regarding claim as to use by developer.	Unknown
Is the technology capable of use in LEA work regarding prevention, intelligence, proactive / reactive detection – (or both).	Reactive only (element of prevention)?
Is the technology capable of use in Overt / covert investigation or both?	Overt (potential for Covert deployment)
Assess effectiveness i.e. Significant / of benefit / minimal / unknown / indeterminable (Go to Website / back to Delft for details if necessary)	Unknown
Any significant Legal / ethical issues?	None
View regarding Level of intrusiveness – high, medium, low, cannot determine.	Low
Cost Effective	Unknown
Any other comments?	

SURVEILLE PROJECT END USER PANEL – INPUT	
NAME OF EUP MEMBER: Full Panel	
Description of Equipment – SOUND – sound processing FIREFACE400	
What category of serious crime does the technology impact on?	Serious crime and CT
Comment regarding claim as to use by developer.	Unknown
Is the technology capable of use in LEA work regarding prevention, intelligence, proactive / reactive detection – (or both).	Reactive only (element of prevention)?
Is the technology capable of use in Overt / covert investigation or both?	Overt (potential for Covert deployment)
Assess effectiveness i.e. Significant / of benefit / minimal / unknown / indeterminable (Go to Website / back to Delft for details if necessary)	Unknown
Any significant Legal / ethical issues?	None
View regarding Level of intrusiveness – high, medium, low, cannot determine.	Low
Cost Effective	Unknown
Any other comments?	

SURVEILLE PROJECT END USER PANEL – INPUT	
NAME OF EUP MEMBER: Full Panel	
Description of Equipment – SOUND – sound recording bug AU046	
What category of serious crime does the technology impact on?	Serious Crime and CT
Comment regarding claim as to use by developer.	The panel feel that the claims regarding performance of this technology will only be achieved if operated in a fully controlled environment. GSM frequency is subject to network coverage and may therefore also be a limiting factor. It is quite possible that ambient noise factors will have an impact on performance quality. The panel consider that additional technology is necessary to record and monitor the product.
Is the technology capable of use in LEA work regarding prevention, intelligence, proactive / reactive detection – (or both).	Both, but limited in performance due to the operational time available of 7 hours. Only limited opportunities for deployment
Is the technology capable of use in Overt / covert investigation or both?	Covert by design however, available for overt use (e.g. Lawful Business Monitoring)
Assess effectiveness i.e. Significant / of benefit / minimal / unknown / indeterminable (Go to Website / back to Delft for details if necessary)	Significant, Could be very beneficial if the operating parameters allow. Therefore the success is based on good environmental factors
Any significant Legal / ethical issues?	There is a high level of legal and ethical issues that can be managed through authorisation of use of this equipment as being justified, proportionate and necessary together with audited use
View regarding Level of intrusiveness – high, medium, low, cannot determine.	High
Cost Effective	Benefits that reduces the time and resources against conventional methods of investigation.

Any other comments?	EUP have limited their assessment and comments to the specific item of technology referred to and not to listening devices in general.

SURVEILLE PROJECT END USER PANEL – INPUT	
NAME OF EUP MEMBER: Full Panel	
Description of Equipment – SPACE – spy sattelites	
What category of serious crime does the technology impact on?	CT with a potential for use in the investigation of serious crime IF a law enforcement agency would be able to access
Comment regarding claim as to use by developer.	Proven regarding visual product – unable to fully assess any claims regarding sound monitoring.
Is the technology capable of use in LEA work regarding prevention, intelligence, proactive / reactive detection – (or both).	Both
Is the technology capable of use in Overt / covert investigation or both?	Potential both but covert use would be expected to be the most common
Assess effectiveness i.e. Significant / of benefit / minimal / unknown / indeterminable (Go to Website / back to Delft for details if necessary)	Of benefit
Any significant Legal / ethical issues?	Audio and video monitoring of another State would certainly involve some legal / ethical considerations. Monitoring of any individual and any private premises for CT or organised crime investigation / operation would also involve some issues and would require the appropriate authorisation.
View regarding Level of intrusiveness – high, medium, low, cannot	The panel considers the level of intrusiveness could range from low to high dependant on the use of the technology and

determine.	the ability of the technology with regard to the level of detail it can detect be it visual or audio.
Cost Effective	Cannot determine
Any other comments?	

SURVEILLE PROJECT END USER PANEL – INPUT	
NAME OF EUP MEMBER: Full Panel	
Description of Equipment – UAV – platform helikite balloon	
What category of serious crime does the technology impact on?	Serious Crime and CT
Comment regarding claim as to use by developer.	Proven
Is the technology capable of use in LEA work regarding prevention, intelligence, proactive / reactive detection – (or both).	Both
Is the technology capable of use in Overt / covert investigation or both?	Both
Assess effectiveness i.e. Significant / of benefit / minimal / unknown / indeterminable (Go to Website / back to Delft for details if necessary)	Significant – but dependent on number of other factors (e.g. weather)
Any significant Legal / ethical issues?	Covert use is dependent on deployment being authorised around justification, proportionality and necessity and the type of sensor
View regarding Level of intrusiveness	Limited due to presence of technology being known to public

– high, medium, low, cannot determine.	however, level will increase if used covertly or on type of sensor
Cost Effective	Significant cost benefits but limited movement
Any other comments?	

SURVEILLE PROJECT END USER PANEL – INPUT	
NAME OF EUP MEMBER: Full Panel	
Description of Equipment – UAV – platform micro helicopter	
What category of serious crime does the technology impact on?	Serious Crime and CT
Comment regarding claim as to use by developer.	Proven
Is the technology capable of use in LEA work regarding prevention, intelligence, proactive / reactive detection – (or both).	Both
Is the technology capable of use in Overt / covert investigation or both?	Both
Assess effectiveness i.e. Significant / of benefit / minimal / unknown / indeterminable (Go to Website / back to Delft for details if necessary)	Significant – but dependent on number of other factors (e.g. weather)
Any significant Legal / ethical issues?	Covert use is dependent on deployment being authorised around justification, proportionality and necessity and the type of sensor

View regarding Level of intrusiveness – high, medium, low, cannot determine.	Limited due to presence of technology being known to public however, level will increase if used covertly or on type of sensor
Cost Effective	Significant cost benefits – considered as more moveable than the balloon but understood to have limited flying time.
Any other comments?	

SURVEILLE PROJECT END USER PANEL – INPUT	
NAME OF EUP MEMBER: Full Panel	
Description of Equipment – X-RAY – luggage screening	
What category of serious crime does the technology impact on?	All serious and organised crime and CT
Comment regarding claim as to use by developer.	Proven technology
Is the technology capable of use in LEA work regarding prevention, intelligence, proactive / reactive detection – (or both).	Prevention, intelligence and pro active investigation
Is the technology capable of use in Overt / covert investigation or both?	Both
Assess effectiveness i.e. Significant / of benefit / minimal / unknown / indeterminable (Go to Website / back to Delft for details if necessary)	Significantly effective

Any significant Legal / ethical issues?	No legal issues. Pre requirement for flights and entry to buildings / locations. Duty to control and safety.
View regarding Level of intrusiveness – high, medium, low, cannot determine.	Low
Cost Effective	Significant
Any other comments?	