MATRIX							
		HUMAN RIGHTS AND ETHICAL ISSUES					
		Moral risk of error leading to significant sanction	Fundamental right to protection of personal data	Fundamental right to privacy or private and family life (not including data protection)	Fundamental right to freedom of thought, conscience and religion	Freedom of movement and residence	Moral risk of damage to trust and chilling effect
TECHNOLOGY AND USE	USABILITY			Moral risk of Intrusion			
1. Visual spectrum dome– zoom, tilt, rotate (public place – used overtly)	6		2	1			
2. Visual spectrum dome– zoom, tilt, rotate (public place – used covertly)	7		8*	2			
3. Covert photography in public place	9		8*	2			
4. Sound recording bug in target's home address.	8		16*	16*			
5. Sound recording bug in target's vehicle.	8		8	6-12			
6. Sound recording bug on public transport used by target.	3		8*	¾*			
7. Sound recording bug in police vehicle transporting target following arrest.	4		8	2			
8. Sound recording bug in target's prison cell.	5		8	4-8			
9. Video camera mounted on platform micro helicopter	6		¾	4-8*		3	
10. AIS ship location detection and identification	5		0	0			
11. Explosives detection near harbor	4			0-¾			
12. Gas chromatography drugs detector	8			0-¾			
13. Whole body scanner eqo	6		0	3			
14. Luggage screening technology	7			0-¾			
15. Money laundering technology	7		8	8	1 ½		
16. Networked data analysis	7		3	2			
17. Data transfer analysis (name recognition) technology	6		8	8	1 ½		

18. Location tracking of cellular phones	7		6	6		2	
19. Mobile phone tap	8		3	8*			

Scores for **usability** run from 0-10, 0 representing the least usable, and 10 the most usable technology. Fundamental rights intrusion scores run from ¾-16, ¾ representing the least problematic interference with fundamental rights, 16 representing the most problematic intrusion. The addition of an asterisk* to the fundamental rights scores indicates that significant third-party intrusion is identified, resulting in a need to justify the surveillance not only as proportionate in relation to the target but also as justified in relation to third parties. Ethical risk assessments are expressed via a colour coding system. No colour is used where the ethics assessment found no risk at all (or a negligible ethical risk). Green indicates a moderate ethical risk, amber an intermediate, and red a severe one.

The main conclusions that in the context of the scenario and the matrix can be drawn from the combination of usability (technology), fundamental rights (law) and moral risk (ethics) assessments of the 19 usage situations of the 14 surveillance technologies can be formulated as follows.

Firstly, there are 7 situations where the surveillance appears as *justified* in respect of a combination of the three different assessments. They are the overt use of CCTV, AIS ship location detection, explosives detection, drug detection by chromatography, body scanners that do not present an image of the actual person, luggage screening, and analysis of open (publicly available) internet data. The security benefit obtained by these methods, represented by the usability score, varies from 4 to 8 (on the scale of maximum 10) with no major fundamental rights intrusion or major ethical risks. One caveat that has to be made also in relation to this category of surveillance technologies is that it must nevertheless be verified that a proper legal basis exists for their use, i.e. that the authority to use these surveillance methods is based on precise and publicly available law. The same caveat will of course apply also in relation to the other categories to be discussed below. A second caveat is specific to the use of open data. While the collection of individual, discrete pieces about a person may not have a strong fundamental rights impact, the aggregation of various types of (unrelated) open sources (from different contexts) in order to build a profile of a person can have a serious fundamental rights impact.

A second group consists of 3 situations where the combination of the three assessments in the form of a matrix gives the outcome that the use of the particular surveillance method in the context of the scenario would be *suspect,* even if one cannot come to a definite conclusion that it cannot be justified. These are covert photography in public space, money laundering detection technology and analysis of Internet data by data crawlers. The usability score varies from 6 to 9, signifying a somewhat higher average security benefit than in the case of the 7 unproblematic technologies. However, the significant risk of intrusion into fundamental rights of third parties appears to outweigh the security benefit of covert photography in a public place. As to the two other technologies in this group, it is the degree of intrusion into the fundamental rights (privacy and data protection) of the actual target that makes them suspect. As the fundamental rights score and the usability score in all three cases are quite close to each other, and as the ethical risks are not particularly high, it can nevertheless be concluded that judicial authorization would make the surveillance justified in these three cases.

A third group of surveillance technology usage situations includes 4 cases where the comparison between usability (security benefit) and fundamental rights intrusion is similar than in the second category, making the surveillance suspect and potentially legitimate if judicial authorization is given. The difference compared to the second group, however, is the identification of significant ethical risk. The four cases are the placement of a sound recording bug in the suspect's vehicle, the use of a micro helicopter for aerial surveillance, location tracking of cellular phones and tapping of mobile phones for retrieving metadata, including a register of the calls or text messages placed or received. The usability score in all four cases is relatively high (from 6 to 8) but so is the fundamental rights intrusion (from 6 to 8 or even 12 when the most deeply affected fundamental right is looked into). Due to the high level of third-party intrusion in two of the cases (micro helicopter and mobile phone metadata tap) and high moral risk in all four cases, here identified as a *highly suspect* category, it is questionable whether even judicial authorization could make the surveillance acceptable. Another way to formulate this conclusion is that the judiciary should be hesitant to authorize these measures if requested, due to the fundamental rights intrusion, third party effect, and moral risk. In some cases it may be possible to mitigate the adverse consequences to reach a solution where judicial authorization would make the surveillance legitimate. Restrictions in time and place in the use of the surveillance, privacy by design features built into the technology for instance to avoid third-party intrusion, or proper representation of the interests of the targeted person in the judicial authorization process may be among the solutions.

The remaining 5 usage situations of surveillance technologies can be identified as legally *impermissible* for various reasons. In the case of covert use of CCTV the outcome flows from the fundamental rights intrusion score (8) narrowly outweighing the clear security benefit (7), but combined with a high level of third-party intrusion. It can be noted that covert photography in a public place fell in the second, suspect, category above, simply because of its higher usability score. The outcome is the same for the placement of a sound recording bug in the suspect's home. The security benefit is quite high (8) but here the level of fundamental rights intrusion is even higher (16), coupled with significant risk of third-party intrusion and also high moral risk. This is a clear case where the matrix suggests that even judicial authorisation cannot justify the surveillance measure and should therefore be denied. As for the placing of a sound recording bug in either public transport (a bus), or in a police car, or in the suspect's prison cell - all three represent a clearly lower level of intrusion into fundamental rights. As, however, also the security benefit is dramatically lower (between 3 and 5), it is with a clear margin outweighed by the fundamental rights intrusion score (8). In all five cases also intermediate or high moral risk was identified. It is suggested that in the case of these 5 situations even judicial authorization could not make the surveillance justified, either due to third-party intrusion, the intensity of the intrusion into the suspect's rights, or the limited security benefit obtained through the measure. Quite often the conclusion to be drawn would be to look for an alternative surveillance method that would yield either a higher usability score or a lower fundamental rights intrusion score (or ideally both), and in addition would not raise a flag of significant moral risk. The placing of the 5 situations in the category of impermissible surveillance, in the context of the scenario, does not mean that the use of the same technologies would by definition always be legally impermissible.

It is to be noted that the assessment was made in the context of a crime prevention/investigation scenario that was neutral in relation to the applicable legal system and the characteristics of the targets, and did not include identifiable third parties. Minor adjustments may be needed to take into account these additional factors. That said, the multidimensional matrix developed here by the

SURVEILLE consortium is a promising step towards developing a methodological tool to assess the all-things-considered costs and benefits of various surveillance technologies to be used for combating crime.

The methodology for arriving at these scores is outlined in section 2.3, immediately below. Then, in 2.4, the matrix is discussed in greater detail, identifying a number of cases where technologies score well on one dimension, but poorly on others.

2.3 Methodologies

2.3.1 Scoring usability

The scoring methodology developed by TU Delft assesses usability on the basis of four factors: effectiveness, cost, privacy by design and excellence. The assessment of the first three of these, effectiveness, cost and privacy by design, in turn relies on three further factors, to give ten factors in total, each receiving a mark of 1 or 0, to give the score for usability from 0-10, 0 representing the least usable, and 10 the most usable technology.

'Effectiveness' in the TU Delft scoring system refers to the technology's ability to increase security by carrying out a specified function within the relevant context.[2] The assessment of effectiveness relies on the three further factors of delivery, simplicity and sensitivity.

'Delivery' refers to whether or not the equipment yields a useful outcome when used correctly. Surveillance technologies vary considerably in their function – sometimes the useful function can be defined narrowly in terms of the detection of a specific prohibited object, such as a weapon, or a contraband substance. Sometimes the useful outcome will refer to gaining access to a private space to assist with ongoing intelligence gathering. On other occasions it may simply refer to providing useful leads for further investigation. Delivering a useful outcome, however, does not imply that the technology is not susceptible to error (an issue addressed by the factor of 'sensitivity', discussed below). Furthermore, a technology may 'deliver' successfully in one context, but fail to do so in another (for example the listening equipment is judged to 'deliver' planted in the suspect's home, but not when placed on public transport).

Simplicity refers to structure and ease of operation. Other things being equal, simpler technologies are more effective. The involvement of more than one external expert or stakeholder is an example of something that might make a technology too complex to score for simplicity. In both the case of 'delivery' and 'simplicity', the criteria for scoring '1' is either evidence of past success, or the fact that that it is reasonable to expect that success is achievable. In the absence of either, the technology scores '0'.

Sensitivity refers to the likelihood of error. Technologies that are awarded a '1' in this category provide information that is clear as well as accurate, and that is not susceptible of multiple interpretations. Where there is evidence that a technology is prone to error it scores a '0', and if there is no evidence available of its clear outputs it also scores '0'. Only if there is evidence of its

[2] "*Effective*: the technology has the technical capacity to deliver increased security, and when employed for a defined goal within the necessary context (good location, trained operators, a larger security system, etc.) achieves the intended outcome." Annex 2.

precise and accurate output does it score '1'. The three scores for 'delivery', 'simplicity' and 'sensitivity' are added to give a score for 'effectiveness' out of three.

The second category contributing to the overall score for usability is cost. This refers to the different ways in which the financial costs of surveillance technology vary. The score for 'cost' is also determined on the basis of three factors: 'purchase cost', 'personnel requirements' and 'additional resources'. Purchase cost is the upfront price of the equipment and associated systems needed to run it. Both identifying prices and selecting a criteria for costliness are problematic. Prices for the same technology will vary for one thing. And more substantially budgets available to policing authorities will vary by jurisdiction. Necessarily a nominal scoring system such as that used for the matrix can only provide limited insight into this issue. Technologies costing €50,000 or more, score a '0', and technologies costing less score a '1'. Personnel requirements refers to the number of people who are needed to operate the equipment within the organisation carrying out the surveillance. Two or less scores a '1', three or more scores a '0'. 'Additional resources' refers to whether personnel external to the organisation are required for operation – whether commercial partners or vendors, which represents a further source of financial expense. If a third party is involved, a '0' is scored. If not, it scores '1'. The score for these three factors are added together to give a score for cost out of three.

The third category contributing to the overall score for usability is privacy by design. The score for this category relies on scores for three further factors: 'observation of persons', 'collateral intrusion' and 'hardware and software protection'. 'Observation of persons' refers to whether the surveillance technology is used to observe people, as opposed to simple objects or substances. Other things being equal, technologies that observe objects or substances are better than those that observe people. Technologies count as observing people when they monitor or record images of individuals, their behaviour or their voices, resulting in a score of '0'. Technologies that record or otherwise surveille either objects, substances, or data score '1'. 'Collateral intrusion' refers to the likelihood of surveilling people beyond the intended target. Technologies that monitor or record only the intended person(s) score '1', technologies that surveille more than the intended target score '0'. 'Hardware and software protection' refers to the difficulty of building in 'privacy by design' features. If it is difficult to do so, it scores a '0'; if it can be done easily it scores a '1'. The score for these three factors are then added to give a score for 'privacy by design' out of three.

One final factor unrelated to the others is 'excellence'. The criteria for excellence is that the technology has proven its usefulness beyond all reasonable doubt, such as is the case with iris-scans and DNA sampling for personal identification. Technologies qualifying as 'excellent' have been proven their usefulness both scientifically and in application to actual crime prevention and investigation. If the technology's excellence has been proven in this way, it scores a '1'. If it has not, it scores a '0'. This score is then added to the composite scores for 'effectiveness', 'cost' and 'privacy by design' to give the overall usability score out of 10.

2.3.2 Scoring Ethics

The colour coding for the moral risks is derived from the tables visualising moral risk developed in the DETECTER project's 10 Detection Technology Quarterly Updates,[3] based on analysis in DETECTER Deliverable D5.2 and discussed in SURVEILLE Deliverable D2.2.

[3] See for example DETECTER Deliverable D12.2.10 available at www.detecter.bham.ac.uk/pdfs/D12_2_10_QuarterlyUpdateonTechnology_10__1_.doc

Invasion of privacy on this view involves penetration of one of three distinct 'zones' of privacy, discussed in SURVEILLE deliverable D2.2, and DETECTER deliverable D5.2.[4] These are bodily privacy, penetrated by close contact, touching or visual access to the naked body; privacy of home spaces, penetrated by uninvited observation in the home or spaces being temporarily used as such, like a hotel room; and private life, penetrated by inappropriate scrutiny of associational life and matters of conscience. Also relevant is the question of whether information uncovered by the initial intrusion is made available to further people, as intrusion is usually made worse by sharing information. Technologies that delete information upon initial use, or do not store information for further viewing preserve the privacy of the surveilled. Cases where the UW team judge technology not to invade privacy at all, or to do so only to a negligible extent, are left blank; moderate intrusions are coded green; intermediate invasions amber; and severe invasions red.

The moral risk of error may derive from any of a number of sources. Firstly, if the information acquired by the technology is susceptible to false positives this will contribute to errors: some information targeted by surveillance technologies is inherently ambiguous and potentially misleading. For example, a private conversation targeted by means of listening devices can easily be misinterpreted.[5] This is distinct from the technology itself producing/generating, or revealing information which may be highly error prone. For example, data mining technologies often involve profiling algorithms that are susceptible to false positives. Some technologies require extensive training and may be vulnerable to errors because of mistakes by the user or viewer. Finally, storage may lead to repeated risks of error as well, either because of risks of data corruption, or simply because a later viewer does not have all the information to put the intelligence stored in its proper context. However the multiple possible sources of error must be considered in the light of whether the person surveilled is subjected to sanction as a result. It is not error in itself that represents a moral problem here. Rather, it is only error that leads to intrusive searches or arrests that is of concern. No risk of error leading to sanction, or a negligible one, results in the category being left blank. A moderate risk of errors leading to sanction is coded green, an intermediate risk amber, and a severe risk red.

The moral risk of damage to valuable relations of trust refers to two categories of social trust eroded by uses of technology. The first category is the trust in policing authorities that may be damaged by what is perceived as excessive, ethically problematic uses of technology.[6] The second category is, interpersonal social trust among the population – damage to this social trust is sometimes referred to as the 'chilling effect'.[7] Damage to both of these kinds of trust result from the perception of at least four morally problematic possibilities on the part of the general public. One, the perception of the intrusiveness of the technology. Two, the perception of error resulting from the technology –

[4] See DETECTER Deliverables D5.2. especially pp. 7-18 www.detecter.bham.ac.uk/pdfs/D05.2.The_Relative_Moral_Risks_of_Detection_Technology.doc and D12.2.1 – D12.2.10 available at http://detecter.eu/index.php?option=com_content&view=section&layout=blog&id=7&Itemid=9

[5] See for example DETECTER Deliverable D5.2., which refers to range of empirical studies on the interpretation of recorded conversations such as (Graham McGregor, in Alan Thomas,1987) and (Graham McGregor, 1990) and (Dore and McDermott, 1982) on the essential role of context in interpreting conversation – which in the case of technologically enabled eavesdropping may not be available.

[6] 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

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

that the error-proneness of technology poses risks of the individual being wrongly suspected. Three, the perception that the technology poses risks of discrimination – either that the technology is disproportionately likely to be used against particular groups, or even that application of the technology may be more likely to cast suspicion on particular groups, as is the case for example with data mining technologies which make use of crude profiling techniques.[8] Four, the perception of function creep also contributes to this damage to social trust. No risk of damage, or negligible damage to relations of trust result in the category being left blank, moderate risk of damage is coded green, an intermediate risk amber, and a severe risk red.

2.3.3 Scoring Fundamental Rights

The scores for fundamental rights, given by the EUI team in SURVEILLE, are closely connected to the use of the technologies in the context of the investigatory scenario from MERPOL. EUI provides assessments of the intrusions the proposed uses of the technologies in the scenario cause to fundamental rights. The assessment relies upon a multitude of approaches, including Robert Alexy's theory of fundamental rights,[9] identification of attributes within a fundamental right in order to assess the weight of the rights in context,[10] and analysis of existing case law, both by the European Court of Human Rights and the Court of Justice of the European Union.

Scores are offered for a number of different fundamental rights, with emphasis on the right to the protection of private life (or privacy), on the one hand, and the right to the protection of personal data, on the other hand. Although these two rights are closely interlinked, the protection of personal data is increasingly conceived of as an autonomous fundamental right in the current state of evolution of European law, related to but distinct from the right to respect for private life. This is neatly illustrated by the EU Charter of Fundamental Rights in which data protection has been enshrined as an autonomous fundamental right in Article 8, alongside the protection of private and family life under Article 7.

The concept of private life is a very broad one in accordance with the case law by the European Court of Human Rights, whereas the right to the protection of personal data largely, albeit not exclusively, constitutes one of the aspects or dimensions of the right to respect for private life.[11]

The concept of private life covers the physical and psychological integrity of a person; it embraces aspects of an individual's physical and social identity. Elements such as gender identification, name and sexual orientation and sexual life fall within the personal sphere protected by Article 8 of the ECHR. Moreover, Article 8 protects a right to personal development, and the right to establish and develop relationships with other human beings and the outside world. Although Article 8 does not establish as such any right to self-determination, the European Court of Human Rights has considered the notion of personal autonomy to be an important principle underlying the

[8] See for example Moeckli and Thurman DETECTER Deliverable D8.1. especially on the German Rasterfahndung: www.detecter.bham.ac.uk/pdfs/D8.1CounterTerrorismDataMining.doc

[9] Robert Alexy, (2002) *Theory of Constitutional Rights*

[10] For earlier SURVEILLE work, see Porcedda, Maria Grazia (2013), 'Paper Establishing Classification of Technologies on the Basis of their Intrusiveness into Fundamental Rights': SURVEILLE deliverable D2.4, Florence, European University Institute).

[11] See Maria Tzanou, The Added Value of Data Protection as a Fundamental Right in the EU Legal Order in the Context of Law Enforcement. PhD Thesis European University Institute, 2012.

interpretation of its guarantees.[12]

Data protection, in turn, is usually understood as referring to a set of rules and principles that aim to protect the rights, freedoms and interests of individuals, when information related to them ("personal data") is being processed (e.g. collected, stored, exchanged, altered or deleted).

The difference between privacy and data protection is also indicated by the fact that not all personal data necessarily fall within the concept of private life. *A fortiori*, not all personal data are by their nature capable of undermining the right to private life.[13]

Aside from the right to privacy and the right to the protection of personal data, several other fundamental rights may also be affected in many cases by the use of surveillance technologies, including freedom of movement, freedom of thought, conscience and religion, freedom of expression, freedom of association or the right to non-discrimination. As the assessments were made in relation to the crime investigation scenario, a consideration of the impact on other fundamental rights beyond privacy and data protection was necessary only in a few cases. In many other cases a remark was nevertheless made in respect of the right to non-discrimination.

Where a technology (or rather the application of a technology) engages a fundamental right, a score is given from 0 to 16 where the value 0 would signify no intrusion whatsoever. In practice, the lowest given score was ¾ representing the best case or the least interference. In one case the maximum score of 16 was the outcome, representing the worst case or the greatest intrusion. Any score above 10 represents an impermissible interference with fundamental rights – one that cannot be justified by any increase in security that may result from the use. This is because the maximum usability score was 10, and no usability score could outweigh or counterbalance a fundamental rights intrusion above the score 10.

The scores generated for each technology are primarily a result of two factors: first the weight, or importance of the particular fundamental right affected in the context of the scenario, and second, an assessment of the degree of intrusion into that right. Each of these two factors is marked as 1, 2 or 4. A score of '1' represents a low, '2' a medium and '4' a high relative weighting of the fundamental right. A score of '1' represents a low, '2' a medium and '4' a high (or serious) level of intrusion into that right. These two scores are then multiplied to give a score from 1 to 16.

The scored variables (weight of a right and the degree of an intrusion), as well as the individual scores given to them, stem from classifications and concepts used in everyday legal practice and argumentation. For instance, the ECtHR has often held that the actual significance of a right and the respective margin of appreciation it allows for member states, depends on a number of factors including the nature of the Convention right in issue, its importance for the individual, the nature of the interference and the object pursued by the interference.[14] These aspects have been addressed in the scoring. Similarly, the differentiation between rights that have weak, medium, or high weight as well as between low, medium and serious intrusions have analogous counterparts in concrete legal argumentation. To give an example, in *Peck v. the United Kingdom*[15], the ECtHR held that the

[12] Pretty v. the UK (Application no. 2346/02), judgment of 29 April 2002, Reports of Judgments and Decisions 2002–III.
[13] See e.g. Case T-194/04 *Bavarian Lager,* judgment of the Court of First Instance of 8 November 2007, paras 118-119.
[14] See for example, S. and Marper v. The United Kingdom (December 4, 2008), § 102
[15] Peck v. The United Kingdom (January 29, 2003), § 63.

disclosure to the media for broadcast use of video footage of the applicant whose suicide attempt was caught on close circuit television cameras constituted a “serious interference” with the applicant's right to respect for his private life. For the purposes of the matrix, this legal outcome is represented in the matrix assessment by assigning the score of 4 to the assessment of the degree of intrusion.

The two scores provided by the assessment of both the weight of the right and the degree of intrusion are then multiplied to give a score from 1 to 16. This score from 1 to 16 may be reduced by the two multipliers. The first is the reliability of the judgements of the weighting and intrusiveness generating the 1-4 scores. The most reliable assessment has a solid grounding in authoritative case law. In this case there is a scoring of ‘1’, and no consequent reduction of the 1-16 score. Where there was not a solid basis of case law to draw upon, the next reliable basis was a consensus among the EUI team of legal experts. In this case a score of ‘¾’ was awarded. This factor was then multiplied by the 1-16 score, thus reducing the final score by a quarter. The least reliable basis was that of a layman’s opinion, which would result in a score of ‘½’, reducing the raw score by a half. In practice each assessment could be made on the basis of solid case law or expert consensus.

The second multiplier that can reduce the 1-16 scoring is judicial authorisation. This reflects the fact that judicial authorisation mitigates the intrusion. However, certain interferences with fundamental rights are so intrusive that even with judicial authorisation they remain unacceptable. In the scoring, judicial authorisation results in a score of ‘¾’, which is multiplied by the raw, 1-16 score, reducing it by a quarter. In the absence of judicial authorisation a ‘1’ is scored for this category, retaining the original assessment. For example, in the case of the maximum original score of ‘16’, even with judicial authorisation this is reduced to 12 – still above the maximum score of 10 that could be counterbalanced by maximum security benefit. As the analysis is carried out in relation to an unspecified jurisdiction, it could not be assessed whether the law would in each case require judicial authorization. Hence, the question of judicial authorization was left open. In assessing real life cases both the existence of appropriate judicial mechanisms and their effective operation would stand in need of verification.

One important precondition for an interference in a fundamental right being permissible is that it was ‘prescribed by law’, i.e. that there was a proper legal basis for it in the applicable legal framework, typically national legislation regulating the investigation of crime and the powers various authorities possess for it. The requirement of any interference being prescribed by law does not merely relate to the existence of law but also to the quality of the law, including its degree of precision and foreseeability. The absence of proper legal basis would turn otherwise permissible surveillance into impermissible surveillance, whenever there is an interference with fundamental rights, including the right to privacy. As the assessment was not made in respect of a particular jurisdiction, the existence of a legal basis for each use of surveillance technologies could not be determined. Instead, it was assumed that legal basis existed and a score was given under such an assumption. In real life situations, the validity of the assumption would need to be verified.

In the scoring as applied, the maximum score of ‘16’ was the result of a combination of the highest level of intrusion into a fundamental right that was of highest weight in the context under analysis (4 x 4 = 16). Although not applied in practice when assessing the scenario, the maximum score of 16 could also be awarded directly under the construction that the surveillance under assessment intruded into the inviolable or essential ‘core’ of a fundamental right. This is because it is one of the analytically distinct preconditions of the permissibility of any interference with a fundamental right

that the restriction in question leaves unaffected the essential core of the right. Further, as some fundamental rights, such as the prohibition against torture, are absolute in the meaning that they do not allow for any restrictions, the maximum score of 16 could also be awarded directly when an intrusion into an absolute right is identified.[16] However, in this deliverable neither of these cases was identified in any of the situations analysed but the scoring could always be given through the two-step separate assessment of the weight of the right and the intensity of the intrusion.

Finally, the scenario as described contains instances where there is potential for 'third-party' or 'collateral' intrusion of individuals beyond the intended target. Therefore these cases would require further and separate legal analysis as to their permissibility, and/or how such third-party intrusion could be prevented. This analysis would require detail beyond the scope of the original scenario. Those cases where a significant risk for third party analysis has been identified are marked with an asterisk (*).

2.4 Discussion of the Matrix

The fundamental rights and ethics analyses should be understood as serving complementary but distinct purposes in the matrix. The former is a legal assessment of uses of the technologies by police forces in the context of an investigation. This analysis is therefore necessarily more tightly bound to the context of the police investigation scenario given below. Both assessments reflect the uses of technologies specified in the scenario. However the ethics analyses technology descriptions in the abstract and not just their uses in the scenario. In part this is due to the difference between the approaches of ethics and law to the technologies.

Ethical and legal analysis overlap to an extent – the legal right to privacy and the moral interest in privacy, for example, share certain features and arguably protect some of the same values: especially that of having an unobserved sphere to develop independent and autonomous thought. This overlap is reflected in the matrix by their sharing a column. The two other moral risks mentioned overlap with human rights not analysed in the matrix. The moral risk of error is related to the fundamental right to non-discrimination. Error-prone technologies can contribute to discrimination when they disproportionately target particular groups. Discrimination can also contribute to error if prejudiced users decide to deploy technologies, or report suspicions without justification. Some human rights have no overlap with any single moral risk, such as the right to data protection. To the extent that data protection can be cashed out in terms of a moral duty, it is likely to be covered by duties to respect others' privacy, or to stop preventable harm resulting from information sharing.[17]

It is important that surveillance technologies are not used in ways that either violate law or violate ethical norms. Taking only the law into account is not enough, because there are a wide range of possible uses of surveillance technologies that most people would agree are wrong, even if there are reasons why they should not be made illegal. An example of this can be seen in the response to revelations about mass surveillance of Internet data on the part of the American NSA and British GCHQ in 2013 where one argument has been that the surveillance might have been legal under domestic law but was nevertheless unethical (and arguably also in violation of international human rights law). Likewise, ethical assessment is by itself insufficient, because some things that are not

[16] For a discussion of the 'core' of fundamental rights and of absolute rights, see SURVEILLE Deliverable D2.4 and the sources identified there.
[17] In some cases this duty might correspond to the moral risk of error.