FP7 – SEC- 2011-284725

SURVEILLE

Surveillance: Ethical issues, legal limitations, and efficiency

Collaborative Project

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

SURVEILLE Paper Assessing Surveillance in the Context of Preventing a Terrorist Act

Extract from SURVEILLE Deliverable D2.8: Update of D2.7 on the basis of input of other partners. Assessment of surveillance technologies and techniques applied in a terrorism prevention scenario.

Due date of deliverable: 31.07.2014

Actual submission date: 29.05.2014

Start date of project: 1.2.2012 Duration: 39 months

SURVEILLE Work Package number and lead: WP02 Prof. Tom Sorell

Author(s) of deliverable D2.8:

The TU Delft team: Coen van Gulijk; Michelle Cayford; Bert-Jan Kooij.

The EUI team: Martin Scheinin; Mathias Vermeulen, Juha Lavapuro, Tuomas Ojanen, Jonathan Andrew, Douwe Korff

The UW team: John Guelke; Tom Sorell and Katerina Hadjimatheou

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

- SURVEILLE deliverable D2.8 continues the approach pioneered in SURVEILLE deliverable D2.6 for combining technical, legal and ethical assessments for the use of surveillance technology in realistic serious crime scenarios. The new scenario considered is terrorism prevention by means of Internet monitoring, emulating what is known about signals intelligence agencies' methods of electronic mass surveillance. The technologies featured and assessed are: the use of a cable splitter off a fiber optic backbone; the use of 'Phantom Viewer' software; the use of social networking analysis and the use of 'Finspy' equipment installed on targeted computers. Non-technological surveillance techniques featured and assessed are the opening of baggage in an airport and the use of a covert surveillance team. The assessments are represented visually in a multidimensional matrix – a grid with numerical scores for fundamental rights risk and technical usability assessments, and colour coding for ethical risk assessment. Deliverable D2.8 was submitted to the European Commission on 29 May 2014. This SURVEILLE Paper, extracted from D2.8, contains the assessments and the resulting matrix as produced in D2.8. As in Deliverable D2.6, the discussion is jurisdiction-neutral, i.e. it does not name any particular EU Member State as conducting the surveillance in question. A separate SURVEILLE Paper, released parallel to this document, contains an assessment and analysis of actual methods of mass surveillance applied by the National Security Agency (NSA) of the United States of America. Minor updates of factual information were made in this extract during August 2014, after the submission on deliverable D2.8 in late May.

- In contrast to the more mixed conclusions of D2.6, the assessments are overwhelmingly critical of the techniques employed: Only the two non-technological surveillance techniques produced usability and fundamental rights intrusion scores and an assessment of possible ethical risks that would make them *justified*, using the same criteria that were used in deliverable D2.6. Three methods of electronic surveillance are assessed as legally *impermissible,* as they resulted in modest usability scores, coupled with the highest possible fundamental rights intrusion score and the highest degree of ethical risk. Only one of the methods of electronic surveillance – social network analysis – is assessed as *highly suspect* (instead of manifestly impermissible), as it produces high scores both as to usability and fundamental rights intrusion, coupled with intermediate ethical risk.

- The methodology underlying the legal assessments is further supported by an analysis of the ruling of the Court of Justice of the European Union on the 8 April 2014 in Joined cases C-293/12, C-594/12 *Digital Rights Ireland and*

Seitlinger and Others[1] that Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC ("Data Retention Directive")[2] is invalid.

- A technical assessment of the techniques used by signals intelligence agencies for mass surveillance remains challenging because the programmes in question are classified. Nevertheless, educated guesswork is possible based on recent leaks, previous revelations, and an understanding of what methods and devices are available. These suggest that the technological basis of mass surveillance is achieved by means of a combination of tapping fiber-optic cables, circumventing encryption, launching cyber attacks, gathering phone metadata, and utilizing traditional spying methods such as bugging embassies and tapping political leaders' phones. The available information on these and other surveillance methods was used as the basis for the terrorism prevention scenario presented in this paper, even if the discussion is presented as jurisdiction-neutral. A parallel separate SURVEILLE paper however describes and assesses the surveillance methods applied by the NSA.

[1] Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v. Minister for Communication et al and Kärtner Landesregierung et al, judgment of 8 April 2014, nyr.

[2] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L105, p. 54)

Table of Contents

§1 Introduction

This SURVEILLE Paper is based on SURVEILLE deliverable D2.8 that both updates SURVEILLE deliverable D2.7 that surveyed surveillance technology, and continues the work of deliverable D2.6 that produced a matrix integrating ethical, legal and technical assessments of surveillance technologies. Earlier, D2.1 provided an initial survey of surveillance technologies for the SURVEILLE project then updated in D2.7, titled 'Update of D2.1 on the basis of input from other partners, while D2.6 introduced a method for combining assessments of the ethical, fundamental rights, and usability aspects of deploying a range of surveillance technologies across the lifetime of a serious crime investigation.

The document begins in §2 with the terrorism prevention scenario. Like the scenario presented in D2.6, this is a fictional but realistic description of a multi stage serious crime investigation, constructed to highlight the use of mass surveillance systems for monitoring online communications, directed against the plotting of terrorist attacks with significant threat to life, and geared towards more targeted action on the basis of the results from mass surveillance. Unlike the D2.6 scenario, however, we do not know exactly what technology signals intelligence agencies employ in such an investigation. The surveillance technology depicted in our scenario is based on what has been revealed regarding the mass surveillance by the United States' National Security Agency (NSA) and other corresponding agencies. We believe our choice of technology to be a realistic supposition, but the reader should bear in mind that the exact kind of surveillance technology used by these agencies and its detailed workings is not known fact. Section §3 then presents a multidimensional matrix incorporating scoring for usability, ethics and fundamental rights (a more detailed alternative matrix is included as an annex which is Annex 2 in the actual SURVEILLE deliverable D2.8). This is followed by the explanations of the three parallel assessments: §4 contains a discussion of the developing ethical considerations at each stage, §5 the technical assessment of the technologies described in the scenario, and §6 a summary version of the fundamental rights assessments (provided in full as Annex 1 of deliverable D2.8 but not reproduced in this extract). In the scenario as presented in this publicly available SURVEILLE Paper, the events are presented as taking place in a non-specified jurisdiction, one Member State of the European Union. As in deliverable D2.6, this choice results in limitations of the fundamental rights assessments as to the specific component of addressing the legal basis of the surveillance measures. The usability scoring follows up from deliverable D2.6 'Matrix of Surveillance Technologies', where human rights infringements and technological usability for surveillance are compared.

§2 Terrorism prevention scenario

1. On the basis of internal and external intelligence reports and other expert assessments, the Government of EU Member State Z. has assessed that the country, including the Government itself, will be facing a threat of international terrorist attacks over a period of several years. The threat of international terrorism is said to come from a diverse range of sources, including Al Qaida and associated networks, and those who share Al Qaida's ideology but do not have direct contact with them. A threat could manifest itself from a lone individual or group, rather than a larger network.

2. The director of the country Z's signals intelligence agency X applies to the competent Minister in January 2013 for a 'certificated interception warrant' authorising the interception of an external communications link, in this case a specific submarine cable crossing a maritime border between country Z and another EU Member State.

3. The agency X uses an "**optical splitter**" on this cable, which duplicates all the data that flow through the cable. The duplicated data are sent to the agency's "Internet buffers", which store all collected content data for 3 days, and metadata (or 'communications data') for 30 days. While the pertinent piece of legislation does not define 'content' as such, it refers to the entirety of the communicated data that are flowing through the cable during one Internet session (i.e. the period where somebody logs on and off the Internet). This encapsulates more than 'traditional' content, such as the content of an e-mail, a text message, a chat message or a phone call), but also a list of all Internet pages a person has viewed, all information one shares through social networking sites like Facebook, all documents edited in "cloud" computing services like Google Docs, etc.). Metadata is 'data about transmitted data'; and consists mostly of 'traffic data'.[3] In this context it refers to data that reveals the means of creation

[3] According to the pertinent piece of legislation "traffic data", in relation to any communication, means—

any data identifying, or purporting to identify, any person, apparatus or location to or from which the communication is or may be transmitted,

of transmitted data, the time and date of its creation, its creator, the location on a computer network where it was created and the standards used. The structured nature of metadata makes it easy to analyze massive datasets using sophisticated data-mining programs, in particular to create 'social graphs' indicating which individuals are in contact with which other individuals over what issues and in what kind of patterns; these graphs and patterns can indicate, for instance, certain operational or hierarchical relationships between various actors.

4. The certificate states that only information that is necessary in the interest of national security can be analysed, such as the fight against terrorism. On the basis of this certificate, the agency makes a list of 'selectors' in March 2013, which can include telephone numbers, e-mail-addresses, certain keywords, but also the use of particular encryption technologies. The stored data can be accessed and searched on the basis of these selectors, which are approved by the Minister and specified in "arrangements" made by him under the pertinent law. Both those arrangements and the specific "selectors" are secret. According to the agency's internal rules, the extracted data are kept in a separate database for five years, for further analysis, while the not-selected data are automatically deleted from the buffer after the above-mentioned time periods.

5. One of the selectors is 'Al Nusra front', the name of a group based in Syria that wants to overthrow the Assad government and create a Pan-Islamic state under Sharia law. The group has claimed responsibility for a number of bombings in Syria in 2012, mostly against targets affiliated with or supportive of the Syrian government, and it is reported that many of its members are also identified as members of Al-Qaeda in Iraq. Al Nusra was listed in the summer of 2013 as a

---

any data identifying or selecting, or purporting to identify or select, apparatus through which, or by means of which, the communication is or may be transmitted,

any data comprising signals for the actuation of apparatus used for the purposes of a telecommunication system for effecting (in whole or in part) the transmission of any communication, and

any data identifying the data or other data as data comprised in or attached to a particular communication,

but that expression includes data identifying a computer file or computer program access to which is obtained, or which is run, by means of the communication to the extent only that the file or program is identified by reference to the apparatus in which it is stored.

terrorist group on the 1267 list by the UN, and on country Z's domestic terrorism list.[4]

6. Another selector is the name of 'Abu Omar', an American convert to Islam who is believed to be fighting in Syria against the Assad government. The US authorities delivered this selector to country Z's signals intelligence agency X and claimed that Abu Omar is suspected of preparing a terrorist attack against the U.S. or one of its major allies - without indicating which intelligence justified this conclusion.

7. In October 2013 Jeroen Pels, a known member of Sharia4C, a vocal Islamist organisation with no ties to Al Qaeda, has returned from Syria. The federal police of EU Member State C interrogate him upon his return. Jeroen Pels claims he worked as a volunteer in a hospital close to the border of Turkey and Syria, but the Federal Prosecutor accuses him of providing material support to Al Nusra. During one interrogation he confirms that he has met Mohamed El Waliki, a high-ranking member of Al Nusra near the border. The Federal Police shares this information with D, the intelligence agency of country C, which shares the name with a number of 'friendly' intelligence agencies, including X, the signals intelligence agency of country Z.

7. An analyst of agency X uses the search function of the **Phantom Viewer** [5] to search for Mohamed El Waliki in the agency's Internet buffer. He finds 170 e-mail-addresses whose inbox contain e-mails that mention the name Mohamed El Waliki. Through **social networking analysis** he makes a social graph of these accounts.[6] These analyses are logged in the agency's notebook. 99% of the analyses don't lead to actionable intelligence. One account appears for instance to belong to a university researcher who is doing research into the main actors of the Syrian uprising, another account is used by Brian, a young hacker who is communicating through commercially available encryption technology with members of the Syrian Electronic Army. Two analyses reveal that two e-mail-addresses (A and B) have been communicating with known selectors. The contact list of e-mail-address A contains a number of contacts of low-ranking Al Nusra members. E-mail address B has received an e-mail from a Hotmail-account that is believed to be used by Abu Omar's right hand man.

[4] The analysis in this paper was concluded before the Islamic State of Iraq and the Levant (ISIL) - also known as the Islamic State of Iraq and Syria (ISIS) or just 'IS' – the 'successor' of al-Qaeda in Iraq, conquered several cities in Iraq and committed crimes against humanity in Syria. See A/HRC/27/60, Report of the independent international commission of inquiry on the Syrian Arab Republic, 13 August 2014.

[5] http://wikileaks.org/spyfiles/files/0/180_TRACESPAN-Phanton-Viewer.pdf

[6] http://wikileaks.org/spyfiles/files/0/207_SS8-SOCIALNETANALYS-201110.pdf

8. E-mail address A is identified as belonging to Sarwar Gunes, a UK resident who runs a pharmacy in London. Gunes has frequently flown to Turkey in the past two years to assist Syrian refugees at the border. During one of these trips to Syria he has met El Waliki, and he talked about this encounter to his wife through e-mail. He is about to arrive by plane from Turkey to country Z. On the basis of intelligence provided by agency X, the national security intelligence agency of country Z decides **to secretly open his baggage** before it goes through to the arrivals hall. Inside they find a fairly uncommon powdered soft drink, Tang, and a large number of batteries. Tang contains a lot of citric acid, which can act as a catalyst for an explosion if mixed with HTMD and hydrogen peroxide.

9. An unknown person uses e-mail-address (B), which contains one e-mail in the inbox that was sent two days earlier from a Syrian IP-address. The e-mail comes from the e-mail address that is believed to be associated with Abu Omar, and tells the owner of account B to ask El Waliki how many Calvin Klein aftershaves he has to carry home for his extended family. The quantities of aftershave he referred to bear a striking similarity to the quantities of hydrogen peroxide that are needed to make an explosive.

10. The signals intelligence agency X passes on this information the Z's national security intelligence agency, who asks for a warrant to put Sarwar Gunes under surveillance. **A surveillance team watches Gunes in an Internet cafe**, researching train timetables for two hours. Gunes regularly frequents four different Internet cafés in his hometown, and uses Skype not only to communicate with his family abroad, including his father Omar Gunes, but also to communicate with some of the people he met at the Turkish border.

11. In November 2013, new intelligence from Turkey suggests that a high profile attack on the Underground of country Z's capital is imminent. The national security intelligence agency obtains a warrant from the Minister to place **Finspy equipment**[7] on all computers in the Internet cafés Gunes visits in order to be able to listen in to his conversations when he Skypes, and to see with whom he chats online. Finspy is only activated when the visual surveillance team confirms that Gunes is using a particular computer and it is only used in relation to the computer and Internet communications used by the target. Gunes often watches speeches in which Abu Omar explains in simple English what 'true jihad' means, and what certain Islamic principles 'really' mean.

[7] http://wikileaks.org/spyfiles/files/0/289_GAMMA-201110-FinSpy.pdf. The analysis in this paper was concluded before a user manual on FinSpy was leaked to the wider public in August 2014. The Finspy user manual can be found here: http://f.cl.ly/items/0n3L150w010K3l0y262Q/0F28548C.pdf

12. The national security intelligence agency shares this intelligence with the Police Counter Terrorism Command, which assess whether Gunes should be taken in pre-charge detention in order to allow the police to obtain, preserve and analyze evidence for use in criminal proceedings, or whether Gunes should be further surveilled instead.

§3 Matrix of Surveillance Technologies and Techniques

The surveillance methods used in the above scenario were assessed by three expert teams in SURVEILLE for ethical issues that arise (§4), for technological usability (see §5) and for resulting fundamental rights intrusion (§6). The assessments were made respectively by the ethics team at Warwick, the technology assessment team at TU Delft, and the legal team at the EUI. The resulting scores are presented here as a summary of the three assessments and explained in detail in the three chapters that follow.

Matrix			
Technologies and techniques	Usability	Fundamental Rights Intrusion	Ethical risks
1. Cable Splitting Fiber optic backbone	5	16	
2. Phantom viewer	5	16	
3. Social networking analysis	8	8	
4. Opening baggage	8	¾	
5. Covert surveillance team	6	¾	
6. Finspy	4	16	

Scores for **usability** run from 0-10, 0 representing the least usable, and 10 the most usable technology. **Fundamental rights** intrusion scores run from 0-16, 0 representing no interference with fundamental rights, 16 representing the most problematic intrusion. **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. An alternative version of the matrix table, detailing the different fundamental rights and ethical risks, may be found in Annex 2.

§4 Discussion of Ethical Considerations Arising in the Scenario (written by the UW team)

Stage 1 The nature of the threat identified by country Z's intelligence assessments is very serious, but also very vague when it comes to identifying actual suspects. The possibility of plots being organised by networks or groups suggests intelligence gathering aimed at intercepting communications between plotters, and pursuing all leads on known links to Al Qaeda networks. For preventing attacks by either individuals or groups, the monitoring of the acquisition of arms or materials that could be used for explosives might be justifiable. Monitoring the acquisition of materials involves intrusion, but intrusion directed at preventing death and serious injury. However the justification for monitoring materials, which have other legitimate uses, has to be weighed against how common such materials are, whether this is a sensible use of intelligence resources and the inconvenience this might pose to innocent people.

Stage 2 Monitoring of private communications – that is to say listening to or reading communications made through an ostensibly private channel, rather than conversations in public places – is highly invasive. It is an invasion that can be justified where there is good reason to suggest that the communication concerns serious criminality. The criminality in question is of the most serious, life-threatening kind. Rather than intercepting a particular message, the signals intelligence agency proposed interception of all information conveyed across a particular submarine cable. Granted that the agency might have good reason to think messages used to plot attacks will be carried on this cable, the overwhelming majority of the information carried by this cable will consist of private messages of no legitimate interest.

Is interception of this information in itself an intrusion? Interception may mean mere collection. From one perspective intrusion requires that that one's messages be read by another, rather than merely collected. From another perspective the mere fact that one's communications are easily viewable by another is sufficient for intrusion, even if the communications are not in fact viewed at all or mined but not viewed in full. However, one of the benefits of private communications is not only that others do not see our communications but that we can have *confidence* in the privacy of our communications. The privacy of my communications is unambiguously violated when somebody else reads them without invitation. I suffer a lesser harm when steps are taken which make my private communications easily accessible to others – for example if somebody steams open my letter prior to its delivery to the intended recipient, regardless of whether it is read or not. However, even though it is a lesser harm, it might still be unjust, for example if there is no evidence of any connection to serious crime.

Intercepting the submarine cable is like being in a position to steam open all the letters coming into the country. Describing this as a system of mass surveillance similar to a

totalitarian regime where all citizens are subject to surveillance is inaccurate, since very few letters of very few people may in fact be steamed open. However, it is reasonable to say that everyone whose communications are intercepted has suffered a harm, since people have a right to have their private communications go uncollected *and* unread, and suffer intrusion when they are collected *or* read. Such a widespread harm could be justified on the basis of a demonstrated security benefit, or on the basis of consent. The claimed security benefit seems fairly modest to date,[8] and the system of tapping directly into cables has been established without the knowledge, and therefore the consent, of the overwhelming majority of the population. Both the ethical and financial costs seem disproportionate to the nature of the threat. It is difficult to argue that the system has been implemented with the consent of the population. Individuals signing contracts with Internet service providers are not made aware that their data may be made available via cable taps to the secret services. The fact that they sign the contract is neither explicit nor tacit consent to such access. Neither can they be said to have consented to such a system through their democratic institutions, because the system has not been approved by any parliamentary body.

Stage 3 The duplication of communications information with the splitter represents a harm to the individuals whose emails these are, albeit the lesser harm of 'collection' rather than of having their correspondence actually read. And this harm may be further limited by deletion after 30 days (obviously this is not the case for those whose data is retained beyond this initial period). Although a lesser and potentially limited harm, this harm can still be an injustice. Can inflicting this harm on such a wide number of people be justified? Certainly it is the case that minor intrusions often are accepted in exchange for some kind of security benefit, such as the widespread acceptance of the screening of baggage and body searches at airports. However, people know about, and can be understood as having consented to these searches as a part of flying, whereas this cannot be presumed to be true of Internet users in general.

Furthermore there are good reasons to value control over our correspondence, such as the fact that our ability to determine for ourselves who we will associate and communicate with is central to moral and political autonomy.[9] This is the means by which we expose ourselves to other points of view and may expose the reasoning that underlies our own beliefs to the scrutiny of others. The privacy of our correspondence is crucial to many people making truly free decisions about which voices to listen, decisions that are not overwhelmingly influenced by powerful figures in the individual's life, whether parents, employers or friends. Furthermore, social networking analysis reveals rich information about an individual's social interactions with others and their relations to groups of people. It might reveal that someone was influential within a

[8] See James Bamford 'They Know Much More than you Think', who argues that in the 50 or so claimed success cases warrants would easily have been granted.
http://www.nybooks.com/articles/archives/2013/aug/15/nsa-they-know-much-more-you-think/

[9] See for example the discussion in (Lever, 2011, 48-50)

group – that a communication from them is likely to result in swift responses and interactions, for example, or that they are peripheral and unlikely to be listened to. Scrutiny of this kind of analysis may certainly be invasive, and require a reason to merit investigation.

Stage 4 In order to justify the establishment of an elaborate system of interception the agency must be able to limit intrusions to just those communications which there is good reason to suspect contain evidence of plots to attack. A certificate stating that 'only information that is necessary in the interest of national security can be collected' appears to restrict intrusions considerably. However, it is highly questionable whether such a restriction can ever be compatible with mass interception of all messages passing through the submarine cable. Even if it was morally justified to look at just a subset, such as 'information necessary in the interest of national security', justifying mass collection will depend on the success of the techniques used to restrict what is actually looked at.

Furthermore, it is possible to question whether gathering all information 'necessary in the interest of national security' might still be too permissive. This is because 'national security' is a vague and disputed concept. It is possible to justify gathering information that is crucial to protecting human beings from serious physical harm, serious injuries and death. Harder to justify is the gathering of information that is pertinent to *economic wellbeing*, which is often included in interpretations of national security. In practice threats to 'economic well being' are often included alongside 'national security' as permitted objectives of intelligence gathering.[10] Life is a condition of a lifeplan, and serious injury has a significant impact on welfare. Protecting human beings can often justify compromising everyday norms of privacy. Preserving the economic performance of already wealthy nations cannot justify intrusions in the same way. Claims in the Brazilian press that Internet surveillance was used by the US to capture commercial secrets in South America's petroleum and energy industries, for example, provide a case of surveillance activity without sufficient justification.[11]

Filtering information on the basis of selectors is potentially a powerful way of allowing access to the genuinely pertinent information while excluding the vast majority of material from intrusive inspection. However, the selectors used are likely in many cases to pick out far more communications than are genuinely useful to investigators. The process of removing material that is not pertinent from further scrutiny ought to be robust.

For example, the use of encryption is applied as a selector. This may seem reasonable, because a desire to conceal the contents of one's communications could be motivated

[10] See for example http://www.legislation.gov.uk/ukpga/1994/13/section/3

[11] See for example http://www.reuters.com/article/2013/07/09/us-usa-security-latinamerica-idUSBRE96816H20130709

by a desire to conceal serious illegality. But huge numbers of people use encryption for other reasons. For example, if a message is encrypted and it originates with a legitimate bank, it could be a simple security measure. The overwhelming majority of people using encryption will be of no interest to counter terrorism authorities. Furthermore, encryption is a completely legitimate step of the political activist seeking to avoid the scrutiny of an authoritarian state – for example the use of Tor software is widely understood to fulfil the function of protecting Internet activity from state intrusion,[12] especially in illiberal states, and people engaged in nonviolent, peaceful political activism should be able to protect themselves against oppressive state interference without coming under suspicion of terrorism or other serious crimes.

Selectors can be objectionable if they are discriminatory. A discriminatory selector might be unreasonably based on prejudice about the likely characteristics of those plotting attacks. The experience of one of the earliest attempts to find terrorist suspects my mining large databases is instructive here. The German Rasterfahndung filtered data Government had access to selecting suspects on the basis of having come from an Islamic country, being registered as a student, and being a male between 18 and 40 years of age. The system was objectionable for producing huge numbers of suspects the overwhelming majority of which are bound to have been innocent (it singled out 300,000 individuals and is not known to have resulted in any arrests at all).[13] It is also objectionable because the selectors are discriminatory, particularly the one selecting for coming from an Islamic country. This is discriminatory because singles out a group of people on the basis of a trait that is not correlated with criminality. As well as directly singling out a group on the basis of a trait like 'having come from an Islamic country', a selector might also disproportionately identify the communications of particular kinds of groups as suspicious – this is sometimes known as 'indirect discrimination. Both kinds of discrimination are objectionable.

The use of keywords is potentially very different from the use of encryption as a selector. However there is great variation in the justification of different keywords that might be used. The ideal selector would be a word that is known to be used exclusively by plotters of a serious crime, like a secret code word. Next best are words that provide a strongly evidence-based reason for suspicion, such as highly specialist explosive materials or other weapons. Bad keywords are terms that huge numbers of people might use for any reason, like 'terrorism' or 'Bin Laden'. It is also bad to use a key word that is discriminatory – one disproportionately likely to cast suspicion on innocent members of particular groups. A discriminatory keyword is bad both because it not indicative of suspicious activity, and thus its use is unlikely to result in successful

[12] See https://www.torproject.org/about/overview.html.en and http://www.theguardian.com/technology/2013/nov/05/tor-beginners-guide-nsa-browser

[13] On this (and a range of other counter-terrorism data mining programmes) see DETECTER Deliverable D8.1. www.detecter.bham.ac.uk/pdfs/D8.1CounterTerrorismDataMining.doc

identification of suspects and also because it may well result in privacy intrusions of large numbers of innocent people. A keyword such as 'Imam' is not only useless because it is so widely used for so many reasons, but is also discriminatory because it is more likely to be used by a Muslim. Keywords used as selectors should be reasonable, evidence-based and not discriminatory.

However, use has to be flexible enough to respond to the fact that forensically aware suspects might seek to avoid directly incriminating language – for example, by avoiding direct reference to suspicious substances, items, groups, or people – so any attempt to definitively construct rules for what selectors would be allowable seems fraught with difficulty, especially if the use of selectors become increasingly subject to public accountability.

Stage 5 The names of specific groups could be good selector, capable of being strongly evidence-based, because names refer to specific groups. Anyone might refer to an abstract concept like Jihad, and huge numbers of people will every day. A much smaller number of people will have met El Waliki or had dealings with Al Nusra. However, the names of groups or individuals could also become more widely used because of their prominence in the press, or because the groups/individuals are involved in legitimate political or associational life. The appropriateness of a selector will be determined by considerations such as how likely plotters and their associates are to be using those terms, the ratio of these to innocent people using the terms, and how easy it is going to be, given the techniques available, to separate the latter from the former once the initial selection has been made.

The name of the organisation known as 'Al Qaeda in Iraq' should also not be used uncritically as a selector. Originally this organisation named itself 'The Islamic State of Iraq and the Levant', and was referred to as 'Al Qaeda in Iraq' in 2004 when its leadership pledged loyalty to Al Qaeda. The organisation has subsequently become an umbrella group of insurgent groups in Iraq and Syria. Membership in an ISIL affiliated group is not the same thing as membership of Al Qaeda. Al Qaeda is unusual amongst even violent Islamist groups in that it pursues violent attacks outside the local theatre of conflict – this feature is why Al Qaeda is such an intelligence priority for American and European agencies. It is not a feature of the organisations that fall under the 'Al Qaeda in Iraq' title.

Stage 6 Although names can be a good selector, many names are common – there are likely to be many 'Abu Omar's. There may as a result be a large number of false positives- innocent individuals whose privacy is invaded because they share a name with or associate closely with people who share a name with the specific suspect. The number of false positives should be factored into any assessment of the proportionality of the intrusion. In addition, name matching in databases is prone to error, particularly

when a name in foreign script is transcribed into the Roman alphabet.[14] Error here is unlikely to be neutral, but will rather most probably direct suspicion and scrutiny at members of a particular ethnic and cultural group, because names are largely culturally inherited.

These risks are exacerbated by the fact that the original intelligence on which the suspicion is based is unknown to the recipients at the signals intelligence agency. Without knowing the original evidence, for example, it will be impossible for the agency to recognise exonerating evidence that would enable them to eliminate Abu Omar from their enquiries. Also, withholding the original intelligence would mask errors (such as name matching errors) that could have taken place earlier, preventing them from being corrected. Because the agency cannot assess and scrutinise the intelligence for themselves, they will have to weigh their uncertainty about its strength against the extent to which they can trust the agency that passed it to them.

Invasions of privacy are wrongs inflicted on individuals. The moral costs of invading a person's privacy has nothing to do with their nationality. Invasions of privacy are wrong because they compromise moral and political autonomy. The moral value of autonomy does not depend on citizenship. Some have responded to the revelations about mass monitoring of global communications by claiming that monitoring of foreign government activity has long been a key function of intelligence services, and an entirely legitimate one. States derive their legitimacy from promoting the interests of their citizens, and these interests compete across different countries. It is true that monitoring of communications relevant to significantly welfare threatening activity is legitimate, and that often such threats have come from foreign governments. However, this does not mean that 'welfare threatening' and 'foreign' are synonymous.

Treating all foreign communications as inherently 'suspect', and thus liable to monitoring is objectionably crude because it fails to distinguish between different kinds of states, between the different possible relations that might exist between different states, and between citizens and their governments. In the case of genuinely 'hostile' countries, even treating all government communications as liable to monitoring fails to recognise how wide a range of activity government employees take part in of no significance whatsoever to the outside world.

[14] See for example 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'

First, most countries do not count as hostile. Foreign countries may be neutral or explicitly allied. Indeed, one particular point of grievance with the mass Internet surveillance system revealed in 2013 is that it has been used against citizens of countries that understood themselves to be 'allies' – why should the telephone of the prime minister of an ally be liable for tapping by America when no plausible scenario exists for that country to threaten any American citizen's welfare, and indeed the two countries are fellow members of NATO? Allies may exist in a state of economic competition, and access to communications of government officials can contribute to a country's ability to promote the interests of its own citizens, not all interests are compelling enough to justify serious intrusion. Welfare must be significantly threatened before such intrusions can be justified: typically violence that threatens life or serious injury. Getting the best possible terms in a trade deal with another country is a legitimate priority for any state government, for example, but not one that could justify monitoring of private communications.

Furthermore, the communications of an overwhelming majority of the citizens of even hostile nations are people of no concern – entirely irrelevant to the interests of other countries however broadly construed. The fact that a particular foreign country is an adversary does not make its citizens adversaries. Even restricting monitoring activity to just those employed by a hostile government seems over wide, as government employs people for such a broad range of functions and the extent of those of possible legitimate interest would be so small – being employed by an adversarial government does not make one an adversary either. The only relevance left to nationality is being employed by a hostile country for adversarial purposes, where 'adversarial purposes' can be spelled out in terms of serious threats to welfare.

Stage 7 Most Islamist groups, although highly criticisable from the perspective of liberal theory, are non violent. Groups may be criticisable because of unjustifiable condemnation of gay people, discrimination against women, as well as hostility to liberal democratic principles such as religious liberty or freedom of speech. This is the case with Sharia4C, which although anti democratic and illiberal has not been found to engage in violence. Al Nusra is an Islamist group that has been a violent combatant in the Syrian civil war, but has never engaged in violence outside this theatre. Evidence of assisting this group should still be treated as a serious matter, and merits police scrutiny. There are laws in many EU Member States against citizens' active involvement in foreign conflicts. There are good reasons for such laws. For one thing, there is a strong presumption against the justification of any violence, regardless of what country it takes place in. Matters may be more complicated in a civil war situation, but here it is reasonable for the policy of the country as a whole to be set by the democratically accountable institutions.

Nevertheless, involvement in foreign conflict is not in itself a strong basis for suspicion of plotting violence in Europe. Sharing this information with other states may be justified by states' interests in discouraging their citizens from participating with violent

groups abroad, but this should not be justified more loosely as 'suspected involvement with a terrorist group'.

Stage 8 At this point it seems open to question why El Waliki is subject to scrutiny. One might argue that Al Nusra's involvement in violence and the overlap of membership with Al Qaeda in Iraq make any member of Al Nusra liable for scrutiny. However, this justification has to be qualified by the fact that Al Nusra's violence has been restricted to the context of a civil war and Al Qaeda needs to be carefully distinguished from Al Qaeda. These facts are significant not because murders in Syria or Iraq are any less morally wrong than murders in Europe, but rather because there isn't a strong basis to believe that Al Nusra would be involved in violence in EU Member State Z, and that is the sole claimed basis for the signals intelligence agency's Internet surveillance – to identify an attack in Z. If the intelligence is merely that El Waliki has met Jeroen Pels this seems a very thin basis for suspicion of plotting violence in Europe.

As discussed above there are additional problems with the use of a name as a selector. There will be many persons sharing the name Mohamed El Waliki, and in all probability the Phantom Viewer will overwhelmingly turn up emails concerning other persons as a result. As the scenario notes, it is also likely that emails actually referring to the El Waliki in question will do so for a range of reasons other than that the writer is in contact with them. Excluding all these false results from further inquiry might seem to require actually reading them, which is an intrusion of an innocent person's privacy. However, if an algorithm is used to select which emails should be opened and read, this has the ethical benefit of preserving some measure of privacy for those excluded by the search. However, the process may be objectionable nevertheless, because the selectors and analytic techniques may be unreasonably error-prone – if it points suspicion at innocent people – or discriminatory – if it points suspicion at innocent people on the basis of their religion, for example.

The fact that A contacts a number of Al Nusra members rather than just El Waliki increases the likelihood that the email between A and B is genuinely an email concerning engagement with the Al Nusra organisation. It does not make it certain, and it reveals nothing about the nature of the engagement. Again, the Al Nusra members may have common names, or may be chance contacts. There is likely to be a degree of crossover between organisations like Al Nusra and Syrian civil society. Agents should be attentive to alternative explanations – even if A is in contact with a network of Al Nusra members this could be for reasons other than violence: legitimate political or other associational activity.

Stage 9 It seems to follow from what we are told of Gunes's mentions of El Waliki to his wife that emails to his wife are flagged up due to their containing the 'El Waliki' selector, and are read. This is highly intrusive, and, for this reason, a significant harm to him.

It is a condition of air travel that we submit our bags to search by appropriate authorities. We understand that the usual norms governing the privacy of our baggage in public places are compromised as soon as we enter an airport. Even a modest basis for suspicion would make a bag search reasonable and proportionate. However, a discriminatory basis could not be acceptable – for example searching all and only the bags of a particular racial background. Furthermore, if the basis for identifying Gunes as a target of scrutiny in the lead up to this point is discriminatory, it will undermine the justification for even this moderately intrusive action. If Gunes's emails were identified as suspicious on the basis of objectionable keywords, then searching his bags on this basis will be like selecting someone for search at the airport because of their Islamic dress.

The discovery of Tang and batteries is not by itself incriminating evidence – their possession may be entirely innocent. For example, pharmacies such as that in which Gunes works often sell powdered soft drinks, many of which alleviate dehydration or fatigue, which can result from travel.

Stage 10 A and B have corresponded about El Waliki, and A's contact list provides further reason for confidence that this correspondence is about the same El Waliki of interest to the signals intelligence agency. Does the request to ask El Waliki about quantities of aftershave give any reason to suspect B of plotting a bombing? A weak basis, though one sufficient to justify continuing to monitor B's email account, and possibly further surveillance of B if they can be identified. The case against A is weaker still.

Stage 11 The email that is the basis of suspicion of Gunes has been found by searching for emails with selectors including 'El Waliki'. The suspicion is primarily based on associating him with an email sent to another address that has received a message from someone linked to Abu Omar. Abu Omar is suspected by US intelligence of plotting an attack, but note that the signals intelligence agency has no means of knowing how strong or reliable American information on Abu Omar is. The links between Sarwar Gunes and Abu Omar stack uncertainty upon uncertainty. The deployment of a surveillance team is quite a resource-heavy commitment, and fairly intrusive even if restricted to surveilling his activities at the Internet café.

There are two ethical reasons why deployment of a surveillance team may be objectionable at this stage. First it may seem disproportionate given the thinness of the intelligence against Gunes: the suspicion is based on association at a third remove from someone else regarded as suspicious (A has communicated with B, and B with C, C is suspected of close association with D, and D is suspected of plotting violence. Second, consent: It may be said that as Gunes is a citizen of Z, he is able to participate in the democratic processes that make the law and gives his consent to the operation of law enforcement and intelligence gathering, subject to the law. However, the argument that he therefore consents to surveillance is undermined by the secrecy of the surveillance

programme. Furthermore, it is proposed here that Gunes should be subject to a significant intrusion on the basis of an intelligence assessment that depends crucially on the American assessment of Abu Omar – an intelligence assessment that the signals intelligence agency is never in any position to properly assess – so any claim that he consents to this surveillance is weaker still.

Stage 12 Finspy equipment is highly intrusive, exposing the full details of the target's Internet activity, content and all. A person's Internet activity will expose both their private correspondence with others, and also interests they may have good reason to pursue anonymously, sharing with nobody, such as controversial political or religious writing. However, it is being fitted to computers being used in a semi public space where the privacy of the conversation is inherently somewhat compromised. Placing this equipment on the computing equipment creates a vulnerability for all users of the equipment. The national security intelligence agency has an obligation to prevent this vulnerability actually resulting in anybody's privacy being violated. However, it is certainly a lesser harm than actually being surveilled.

For the first time there is a tangible link between Gunes and Abu Omar. However, the nature of the link is still a weak one. Gunes has not been shown to be in contact with Abu Omar, but merely to have listened to some of his speeches. While 'jihad' is a term which some do use to refer to terrorism, it is a common enough term in Islam, and an interest in the concept is very weak evidence that someone approves of violence, let alone intends to carry out violent attacks.[15]

Stage 13 Suspicion that somebody is plotting serious crime presents policing authorities with a difficult question: whether it is better to wait and gather more information, or better to disrupt a plot in progress. Disruption could be carried out by arresting a suspect on the basis of the information one has, even while knowing that a conviction is unlikely. But disruption might also more modestly involve confronting a suspect with evidence against them. Disrupting plots has the disadvantage that convictions may fall through due to a lack of evidence that might well have been gathered had a plot been left to progress. However, disruption is often ethically much easier to reconcile with a liberal state's ethical and human rights commitments. Typically disruption does not involve violation of a suspect's rights, and provides an opportunity for suspects to respond to an accusation, to point to evidence that might demonstrate their innocence, for example. Even arresting somebody on quite a thin evidential basis can be justifiable where it can prevent serious injury and death.

[15] For a thoughtful discussion of the meaning of Jihad in Islamic thought see Ali and Rehman 'The Concept of Jihad in Islamic Law' Journal of Conflict & Security Law (2005), Vol. 10 No. 3, 321–343. For criticism of previous misunderstandings of 'Jihad' see Peirce, Gareth. 'Was it Like this for the Irish?' in The London Review of Books. 2008. vol. 30

Pre-charge detention adds an ethical difficulty if it is unreasonably lengthy. This would be particularly difficult to justify in this instance considering how thin and circumstantial the nature of the intelligence against Gunes is. Arresting Gunes on the thin basis available might be reasonable and proportionate, given the seriousness of the offense and interest in disruption. Holding him for, say, a month is not. Continued surveillance is easier to justify than a lengthy period of pre-charge detention, although this will involve further intrusion of Gunes's privacy, and also foregoes the preventive power of disrupting Gunes, if he is indeed in the process of carrying out a plot.

§5 Usability scoring for the Terrorism prevention scenario

The terrorism prevention scenario in §2 describes a possible prevention scenario. Several technologies and manual operations are mentioned. They are scored according to the usability scoring method described in deliverable D2.6.

§5.1 Scoring table for the Terrorism prevention scenario

Table 1 is the scoring table for the technologies in this scenario. Note that the opening of luggage and observation of a suspect with a team of observers are operations rather than technologies; nevertheless, they can be scored with the usability score described in deliverable D2.6.

		EFFICIENCY			COST			PRIVACY B-D			EX.
TECHNOLOGY AND USE	SCORE	#1	#2	#3	#4	#5	#6	#7	#8	#9	#10
Optical splitter (3)	5	1	0	0	0	1	0	1	0	1	1
Phantom viewer (8)	5	1	1	1	1	1	0	0	0	0	0
Social network analysis (9)	9	1	1	1	1	1	1	1	0	1	1
Baggage opening (9)	8	1	1	1	1	0	0	1	1	1	1
Covert observation (10)	6	1	0	1	1	0	1	0	0	1	1
Finspy equipment (12)	4	1	0	0	1	1	0	0	0	0	1

§5.2 Explanation of scores in the scoring table

§5.2.1 Optical splitter

An optical splitter is a technical device that splits fiber-optic cables that carry information. In this case, the fiber-optic cable is part of the 'backbone' of the internet where massive amounts of data are transported across oceans. These cables are so-called large-volume cables. Basic technological knowledge about splitter technology is available in §7 of this report. In the current scenario, the information that is tapped from the Internet is immediately analyzed with a data-crawler to reduce the amount of data that has to be stored. These functionalities are combined for a single usability score in this scenario.

ATTRIBUTE #1 (EFFICIENCY): DELIVERY

Delivery is almost guaranteed by cable splitting with subsequent data crawling. The cable splitter copies the information that flows through the fiber-optic cable indiscriminately. The selectors make sure that the entirety of the data flow is limited to information that contains the selector words. Typically, the number of selectors is large, compensating for typos and abbreviations. When the right selectors are used relevant information is almost certainly captured unless the terrorists use smart coding. Even after the selection procedure, the amount of data is still very large, making it very likely that the relevant data is captured. Therefore, a score of 1 is justified.

ATTRIBUTE #2 (EFFICIENCY): SIMPLICITY

There is nothing simple about placing a fiber optic splitter in large data carriers. The equipment typically requires a dedicated electrical power system and air-conditioned housing. Since data is stored, it also requires massive storage capacities that, again, require a lot of electrical power and dedicated housing. It is unlikely that a single crime investigation justifies this kind of activity. In addition to that, choosing proper selectors and crawling through large amounts of data that subsequently have to be interpreted by humans is a difficult and laborious process that is far from simple. The score is 0.

ATTRIBUTE #3 (EFFICIENCY): SENSITIVITY

The sensitivity of this method is low; it is aimed at gathering ALL information related to specific selectors. The actual information that is sought for may be minute; a single statement, a single e-mail or connection. Therefore this method scores 0 for sensitivity.

ATTRIBUTE #4 (COST): PURCHASE COST

Initial purchase cost for a fiber optic cable splitter is significant. The leaks by Snowden indicate that this required additional facilities, such as housing, for this kind of activity. Also, software that uses selectors for juridical purposes is not cheap. Nation states develop their own software or adapt to local juridical conditions from vendors or befriended nation states. These technical development costs are significant, if not formidable. It scores 0 on the usability score.

ATTRIBUTE #5 (COST): MANPOWER

Once the splitter and software are installed, they run automatically. Some technical support may be required but it is unlikely that it takes more than 2 people to operate the data extraction process. It scores 1 on the use of personnel. Note that the upkeep of a massive data storage system could require more personnel but those people are not crime-investigators.

ATTRIBUTE #6 (COST): EXTERNAL PERSONNEL

The installation of a fiber-optic splitter is a complex matter that can only be done by technical specialists. Therefore it requires external parties to install and operate. This attribute scores 0 on this element of cost.

ATTRIBUTE #7 (PRIVACY): SUBJECT

Data crawlers select and copy digital data from ALL stored data to a subset of data that contains the part of that data that is deemed more relevant; in that sense, it observes a virtual object. Therefore it scores a 1 on this attribute of privacy by design.

ATTRIBUTE #8 (PRIVACY): COLLATERAL INTRUSION

The collateral intrusion is massive for fiber optic cable splitting with subsequent data crawling. In fact, ALL communication data is tapped and analyzed. Although the data-crawler reduces the amount of data stored, because the splitter copies all the data these combined functionalities score 0 on collateral intrusion.

ATTRIBUTE #9 (PRIVACY): PRIVACY-BY-DESIGN

Even though lots of information is stored it would be relatively easy to incorporate privacy-by-design principles. The time limits to storage, the elimination of data that does not contain selectors and anonymizing non-suspects are all possible. It is unknown whether such privacy-protection measures are in place but from a technological point of view it is possible, therefore attribute 9 scores 1.

ATTRIBUTE #10: EXCELLENCE

Fiber-optic cable splitting is a relatively routine operation in normally operating networks. Therefore, the technology is well known and widely applied. In that sense, it is a proven technology. Selection of data is a relatively widespread activity that is useful for many purposes – it is used in Internet searches and by search engines to recover files from PCs. The success of this technology has to be marked as ‘excellent’ from a technological point of view. Attribute 10 scores 1.

The overall score for cable splitting is 5; it is a relatively straightforward copying function where selectors search for relevant information. The technical capabilities for doing that are relatively difficult but it is an automated system, which in theory does not require the constant attention of analysts or law enforcers. Note that privacy-by-design rules

are possible but not necessarily installed; if they are not installed, the usability score drops down a point to 4.

§5.2.2 Phantom viewer and local splitter

Phantom viewer is a commercial product to support inspection of communication through IP communications (computer to computer). The software (the viewer) is combined with a data splitter for fiber optics or ADSL that has to be physically installed near the target's network. The target is relatively small scale, that is to say, the data that the splitter can handle is typically oriented toward a single Internet connection to serve a house or small office building. Further information is available through the website of the vendor.[16]

ATTRIBUTE #1 (EFFICIENCY): DELIVERY

It is very likely that the technology yields relevant information about a suspect. All their communications are intercepted and can be analyzed. It scores 1 on attribute 1.

ATTRIBUTE #2 (EFFICIENCY): SIMPLICITY

The technology is easy to use. Once the splitter is installed it, the software enables easy access to all information sent through the Internet, including IP-telephone, e-mail, graphics etc. The ease of use scores 1.

ATTRIBUTE #3 (EFFICIENCY): SENSITIVITY

Since the information gathering system is relatively straightforward, it is relatively easy to prevent misinterpretation; that is to say, it is relatively unlikely that an error is made in the gathering of information from a targeted person. This attribute scores 1.

ATTRIBUTE #4 (COST): PURCHASE COST

The purchase cost for this technology is estimated to be low. The splitters are relatively simple pieces of equipment and the software is commercially available and well developed. It scores 1.

ATTRIBUTE #5 (COST): MANPOWER

Though the investigation is performed by a crime-fighting team, a single person can operate the system. Score 1.

[16] http://www.tracespan.com

ATTRIBUTE #6 (COST): EXTERNAL PERSONNEL

The installation of the splitter most probably requires the assistance of the network service provider. In theory it is possible to do this without the provider but this may cause legal problems. For that reason this attribute scores 0.

ATTRIBUTE #7 (PRIVACY): SUBJECT

The software gathers digital data including real-time personal calls and video conferencing; therefore it scores 0 on the observed subject.

ATTRIBUTE #8 (PRIVACY): COLLATERAL INTRUSION

Collateral intrusion is likely. Even when a single Internet connection is surveyed, say to a house or to an office building, it is possible that more people use the Internet connection. Other users of the network are observed automatically. The collateral intrusion score is 0.

ATTRIBUTE #9 (PRIVACY): PRIVACY-BY-DESIGN

The software could be developed to include privacy-by-design rules. However, the information flyer does not indicate that such efforts were taken. This also scores 0.

ATTRIBUTE #10: EXCELLENCE

It is difficult to assess whether this technology should be marked as 'excellent'. Clearly, the package is well developed and police forces are experienced in using it but it is not so clear to what extent this specific program is an industry standard. For that reason it scores 0 on excellence.

Phantom viewer scores a 5. It is an intrusive tool that works much the same way as the cable splitter on the backbone of the Internet but it targets local networks that suspects use. Also, it is employed in a local investigation so that information about the suspect does not travel far. When privacy-by-design rules are implemented and the installation of the splitter can be done without the knowledge of the Internet provider, the score increases to 7.

§5.2.3 Social network analysis

Social network analysis is fundamentally different from data crawling. The starting point for this analysis is to develop mathematical representation of the relations between persons. In this case the relation that a suspect has with other people.[17] Information may be inserted from Internet sources (such as data crawling inspection) from databases or from information gathered through persons. If digital search engines are

[17] Scott, J.G. (2000) Social network analysis, a handbook (2nd ed.) Sage, London.

used, the selectors are persons; this is fundamentally different from arbitrary searches where the selectors may be terms such as ‘terror’ or ‘bomb’.

ATTRIBUTE #1 (EFFICIENCY): DELIVERY

The primary purpose of such software is to facilitate complex network building. It makes the analysis easier and thereby supports ease-of-use. Therefore this technology scores 1 on ease-of-use.

ATTRIBUTE #2 (EFFICIENCY): SIMPLICITY

This software requires some training but it mostly supports an analysis that is already relevant in an investigation. Moreover, software packages that support network analysis have existed for decades, simply to support a task that is already important in crime investigations. Therefore, this technology scores 1 on simplicity.

ATTRIBUTE #3 (EFFICIENCY): SENSITIVITY

The sensitivity of this method is intermediate; it is aimed at gathering information about relations to a person or persons. Those relationships can be analyzed relatively quickly and non-essential relations (with innocent people; or the content of the communication) can be eliminated relatively easily. The sensitivity decreases as more ‘steps’ from the central persons are investigated (2^{nd} order, 3^{rd} order relation in the chain). Though there is no clear data about the rate of success, the almost automatic use in serious crime investigation suggests that this is a sensitive tool. It scores 1 on sensitivity.

ATTRIBUTE #4 (COST): PURCHASE COST

It is unclear just how costly it would be to purchase software of this type. An elaborate analysis system may be costly but relatively simple (or somewhat aged programs) are expected to be cheaper than €50.000 in purchase cost. Therefore it scores a 1 on purchase cost.

ATTRIBUTE #5 (COST): MANPOWER

The use of social network analysis technology does not require more than one analyst or employee. It scores 1 on number of personnel involved.

ATTRIBUTE #6 (COST): EXTERNAL PERSONNEL

Once the software is installed, no external personnel is required to perform the analysis. It scores 1 on attribute 6.

ATTRIBUTE #7 (PRIVACY): SUBJECT

The analysis system deals mostly with names of persons only, and therefore scores 1 on the first element of privacy.

ATTRIBUTE #8 (PRIVACY): COLLATERAL INTRUSION

It is a point of long-standing debate whether investigation of information in the public domain classifies as intrusion at all. It can be argued that because the information is public there is no collateral intrusion in using it in an investigation. If it is argued that using this information still constitutes collateral intrusion, then there is a significant amount of collateral intrusion with social network analysis since ALL relations to the suspect are investigated. The intrusion is not arbitrary (such as with cable splitting) but still relatively extensive. In this case, social network analysis scores 0 on attribute 8.

ATTRIBUTE #9 (PRIVACY): PRIVACY-BY-DESIGN

From a technological point of view, it is relatively easy to incorporate technical means for privacy-by-design. Non-essential relationships can be eliminated quickly and all information about them can easily be erased. The score is 1.

ATTRIBUTE #10: EXCELLENCE

Since technologies to map social interactions between suspect individuals have been around for at least two decades and are used in all serious crime investigations, this technology scores 1 on excellence. Note that newer versions of software may include data crawlers; these extensions to the programme are less well known but primarily contribute to capabilities that were already known.

Due to the focus on suspect individuals and use of a limited set of data, the overall score for social network analysis is 9. The fact that similar analysis have been used by police forces for decades and that there is a significant scientific body-of-knowledge about social network analysis increases the usability of this technology. When data-crawlers are embedded in the software, the tool becomes much more intrusive since it starts analyzing Internet communications. In that case, the score can drop down to 7 because real-time communications may be tapped into and privacy-by-design becomes a lot harder.

§5.2.4 Baggage opening

The opening of hold baggage in airplanes is a relatively straightforward operation. Typically, baggage is tagged for a flight to ensure a smooth-running operation for loading and unloading airplanes. Hold baggage systems may be relatively complex technologies but inspecting a bag that is identified as belonging to a person is straightforward.

ATTRIBUTE #1 (EFFICIENCY): DELIVERY

Opening an individual's travel bags yields immediate results. That is to say, that a trained operator will be able to spot suspect goods relatively easily. It scores 1 on attribute 1.

ATTRIBUTE #2 (EFFICIENCY): SIMPLICITY

Opening luggage is a straightforward operation. There may be locks on the luggage but they are simple locks. If the lock is a TSA lock, it can be opened with a TSA key. The ease of use scores 1.

ATTRIBUTE #3 (EFFICIENCY): SENSITIVITY

It is relatively unlikely that an error is made in the gathering of information from a targeted person's luggage. That is to say, suspect goods can easily be identified. This attribute scores 1.

ATTRIBUTE #4 (COST): PURCHASE COST

There is no purchase cost associated with luggage opening. It scores 1.

ATTRIBUTE #5 (COST): MANPOWER

Though a single person or a pair of persons open the luggage, for speed, it may be necessary to have a team with several specialists. Also, the team would have travel to or be present at the airport. The method is not suited for inspecting many pieces of luggage because the process is labor-intensive. It scores 0.

ATTRIBUTE #6 (COST): EXTERNAL PERSONNEL

Airport personnel will have to participate in finding the right luggage and assisting the operation. For that reason this attribute scores 0.

ATTRIBUTE #7 (PRIVACY): SUBJECT

The person himself is not observed but his or her personal belongings are investigated. However, since air travelers implicitly know that their luggage may be inspected, it scores 1.

ATTRIBUTE #8 (PRIVACY): COLLATERAL INTRUSION

Unless a mistake is made in selecting the luggage, there is no collateral intrusion whatsoever. Only the suspect's luggage is inspected. The collateral intrusion score is 1.

ATTRIBUTE #9 (PRIVACY): PRIVACY-BY-DESIGN

Privacy-by-design may be embedded in the operational procedures for opening luggage. For instance, the investigating team may be limited to two individuals and in absence of airport personnel. So luggage inspection scores 1; it can be designed to protect the suspect's privacy. Also, the information about the findings may be distributed to a limited number of investigators. Though this scenario is possible, it is unlikely that privacy-by-design rules are invoked because the investigators wish to learn as much as possible from an individual's luggage.

ATTRIBUTE #10: EXCELLENCE

Airport staff performs this operation on a routine basis when they believe a suitcase may contain suspect goods. In that sense, the method is tried and tested. It scores 1 for usability.

Luggage inspection scores an 8 in usability scoring. It is a straightforward operation that is easily executed and targets only the subject. It is a relatively labor-intensive method that requires third parties to cooperate. The privacy of other travelers is protected and privacy-by-design rules can be applied for luggage opening. In abiding by air transport regulations, air travelers implicitly agree that their luggage may be investigated.

§5.2.5 Covert observation

The observation of an individual in a public space is a directed covert surveillance operation that does not actually require technology. Such an operation may be supported very effectively by technologies such as sound recording and CCTV cameras. In this case, however, they are not incorporated.

ATTRIBUTE #1 (EFFICIENCY): DELIVERY

Though it is possible that relevant information is found by directed covert surveillance, success depends on careful planning of the operation. If the operatives are well instructed and know what they are looking for, it may not be hard to find relevant information. It scores 1 on attribute 1.

ATTRIBUTE #2 (EFFICIENCY): SIMPLICITY

A directed covert surveillance operation has to be planned and executed carefully. Success may depend on the experience of surveillance operatives and resources that the team is allowed to use. In that sense, such an operation is not a simple task, even if it is a routine one. The ease of use scores 0.

ATTRIBUTE #3 (EFFICIENCY): SENSITIVITY

Since trained operatives that know what they are looking for perform the observations it is unlikely that they misinterpret the information gathered through the targeted surveillance operation. It may take some time before relevant information is revealed but once it is observed, it is easily identified and therefore sensitive. This attribute scores 1.

ATTRIBUTE #4 (COST): PURCHASE COST

There may be purchase costs associated equipment to facilitate a directed covert surveillance operation. Team members may require specialized communication devices. This equipment is not exceedingly expensive. Purchase cost scores 1.

ATTRIBUTE #5 (COST): MANPOWER

Setting up, executing and processing results from a covert surveillance operation requires significant manpower; certainly more than 2, therefore it scores 0 on the usability score.

ATTRIBUTE #6 (COST): EXTERNAL PERSONNEL

A surveillance operation may be labor intensive but when it is performed in a public space, it does not necessarily require external personnel to execute. Therefore it scores 1 on the usability score.

ATTRIBUTE #7 (PRIVACY): SUBJECT

A person is constantly under observation by operatives; that makes a directed covert surveillance operation intrusive by definition. It scores 0.

ATTRIBUTE #8 (PRIVACY): COLLATERAL INTRUSION

For directed covert surveillance operations in an Internet café, collateral intrusion is inevitable. Since the individuals surrounding the target are also observed, the intrusion to their privacy is relatively strong. The collateral intrusion score is 0.

ATTRIBUTE #9 (PRIVACY): PRIVACY-BY-DESIGN

Privacy-by-design rules may be applied in surveillance operations. For instance, recording or reporting non-essential information may be reduced to a minimum and the findings may be limited to a few persons. Therefore, it scores 1 on usability scoring.

ATTRIBUTE #10: EXCELLENCE

This investigation method may be the most traditional of all. It has been tested and tried for more than a century and can only score 1 on excellence.

Directed covert surveillance scores 6 on the usability score. It is a traditional form of surveillance that, in the case of a terrorist investigation, requires planning and preparation and is highly intrusive to the subject and the people surrounding him or her. Note that the level of collateral intrusion may be different for each observation; if only a few bystanders are affected it might be worth considering to score 1 on the collateral intrusion attribute to end up with a score of 7.

§5.2.6 Finspy

Finspy is a networked digital spying tool. It is organized in a similar way as the Internet itself; there is a backbone of relay stations from which users purchase Finspy services. The user purchases a license for spying on a specific target or a larger ‘master’ system that allows for a larger number of targets on different locations. This is in contrast with the phantom viewer that is exclusively installed for spying on small systems; also, Finspy

has more capabilities than Phantom viewer: the camera and microphone can be remotely switched on and off, data on the disk drive can be read, there is an inbuilt keylogger (that records all keystrokes) and an automated code cracker for encrypted files. Further information is mainly available through Wikileaks.[18]

ATTRIBUTE #1 (EFFICIENCY): DELIVERY

As all digital spying programs, the probability that useful data is found this way is relatively high. Large volumes of data are analyzed and the probability that relevant information is in there is significant. Attribute delivery scores 1.

ATTRIBUTE #2 (EFFICIENCY): SIMPLICITY

Though the deployment of the software for a user is relatively straightforward, the Finspy network is a complicated network. In that sense it is not a simple system. It scores 0 for simplicity.

ATTRIBUTE #3 (EFFICIENCY): SENSITIVITY

The technology is not very sensitive. It records much data relatively arbitrarily. According to the brochure on Wikileaks there are filters but it is unclear just how well they work. Finspy scores 0 on sensitivity since the large volume of information may lead to wrong conclusions. Although the technology is used in a targeted manner in the scenario, the score reflects the sensitivity of the technology as a whole.

ATTRIBUTE #4 (COST): PURCHASE COST

The Finspy system cannot be bought. It is owned by GAMMA. Services can only be purchased through licenses. It is thought that a license for investigating a small group (so a single license) would be relatively cheap but a 'master' network probably costs more than €50,000. For the current investigation targeted on relatively few individuals, the cost is probably cheaper than €50,000 so it scores a 1 in purchase cost.

ATTRIBUTE #5 (COST): MANPOWER

A single person can probably use the technology and do the analysis based on the software application. Therefore, Finspy scores 1 on this attribute.

ATTRIBUTE #6 (COST): EXTERNAL PERSONNEL

Finspy depends on the network owned by GAMMA. Therefore, it requires external persons by definition. The technology scores 0 on external contracting.

[18] http://wikileaks.org/spyfiles/files/0/289_GAMMA-201110-FinSpy.pdf

ATTRIBUTE #7 (COST): SUBJECT

As with all data investigation technologies, Finspy mostly observes data; however, it can also be used to film the subject or to listen to their conversations. This makes the software very intrusive. It scores a 0 on object of the intrusion.

ATTRIBUTE #8 (COST): COLLATERAL INTRUSION

Collateral intrusion is very likely since all communications are monitored. The technology scores 0.

ATTRIBUTE #9 (COST): PRIVACY-BY-DESIGN

The software enables filters; these filters could be privacy-by-design applications but the brochure mainly states that it is easier for the analyst because he or she does not have to analyze all data on the subject. It scores 0 for privacy-by-design.

ATTRIBUTE #10 (COST): EXCELLENCE

Finspy is different from Phantom viewer, where relatively small-scale products are sold to users. The Finspy system relies on a fairly complicated and extensive network of internet applications and hardware. This investment is probably very costly but justified. Therefore it appears to be relatively well-established technology. It scores 1 on excellence.

Finspy scores 4, which is a lower score than the Phantom viewer. The lower score is explained by the dependency on a global network that is owned by a commercial party and taps into the Internet at will. Well-designed privacy-by-design rules could raise the score by 1 point.

§5.3 Conclusion

The usability analysis of the technologies in the Terrorism prevention scenario shows that some operations are very useful and focused on the subject. Social network analysis and baggage opening, particularly, score high. The social network analysis is just a software application for an otherwise widely-accepted scientific analysis method that is also used for shops, companies and in operating rooms. Baggage opening is an extremely dedicated operation that only targets the suspect and provides relevant insight in a straightforward manner.

Also, it is demonstrated that many electronic methods are relatively well established and score 1 on ‘excellence’. This is mainly due to the fact that the technologies typically have an alternative, more benign, application: cable splitting and social network analysis are examples of this.

Finspy and the Phantom viewer are comparable products in the sense that they deliver similar information. The Finspy system is much less desirable because it involves an international network that is owned by a private party; law enforcers are not the only

ones that can see the data. Both methods are very intrusive and provide little protection against collateral intrusion: phone calls and video information can be accessed in real-time. Note that both of these technologies depend on networks; once the costly infrastructure for data tapping is installed, future investigations become relatively easy.

Cable splitting of the fiber-optic backbone of the Internet does largely the same thing as Finspy and the Phantom viewer, but on a behemoth scale. Truly immense amounts of information from people around the world are copied and analyzed. Also, the data-crawling function is much less dedicated to individual suspects. Rather all communications related to some selectors are deemed suspect. In that respect, the concept of backbone-splitting makes everyone a suspect.

The usability scoring of operations – baggage opening and directed covert surveillance – score relatively high in this scenario. Especially baggage opening is a targeted action where privacy matters are relatively well covered. Depending on the exact execution of such an operation, the usability score can vary by one or two points.

The precise way in which a technology is deployed can change the usability score of a technology. Most technologies that tap into data-stream can be designed to abide by privacy-by-design rules, which raises their usability score. This is technically feasible but for Phantom Viewer and Finspy there is no evidence that such steps were taken.

§6 Fundamental Rights Scoring

§6.1 Introduction

Earlier SURVEILLE deliverable D2.6 was a scenario-based assessment of 14 surveillance technologies applied in 19 different situations in the context of the detection and investigation of serious organised crime. The resulting usability scores ranged from 3 to 9 on the scale of 0-10, where a higher score reflects better effectiveness and efficiency delivered by the use of a technology, towards a legitimate aim such as the investigation of crime. The same technologies were assessed as to their intrusiveness into fundamental rights, and the scores obtained varied from 0 (no intrusion) to 16, the latter representing the highest possible degree of intrusion. Further, the technologies were also reviewed for their ethical implications using three colours for different degrees of ethical risk: green for moderate, amber for intermediate and red for severe ethical risk.

The outcome of the scoring exercise in deliverable D2.6 was that in seven out of the 19 situations the surveillance appeared as *justified* in respect of a combination of the three different assessments. In these cases, surveillance was given a high usability score, combined with no major fundamental rights intrusion or major ethical risks. Three situations were categorised as *suspect* when a high usability score was coupled with significant fundamental rights intrusion but no significant ethical risk. Another four situations were described as *highly suspect*, because of a high degree of fundamental rights intrusion coupled with significant ethical risk. The two subcategories of suspect use of surveillance were identified as an area where judicial authorization might make permissible an otherwise problematic form of surveillance – at least for purposes of the law. Finally, five of the 19 usage situations of surveillance technologies were assessed as legally *impermissible,* typically because the fundamental rights intrusion score was clearly higher than the usability score, including two cases where the fundamental rights intrusion score was higher than the highest possible usability score.[19]

SURVEILLE deliverable D2.8 builds upon the methodology developed for deliverable D2.6, this time in the context of a terrorism prevention scenario and the use of six surveillance technologies or techniques. In this SURVEILLE Paper extracted from deliverable D2.8, the scenario and analysis are presented as jurisdiction-neutral, as was done also in deliverable D2.6. After the completion of deliverable D2.6 and while the SURVEILLE consortium was working on current deliverable D2.8, the highest EU court, the Court of Justice of the European Union (CJEU), issued its ruling in *Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others*,[20] declaring invalid

[19] These two situations were the placing of a sound recording bug in the target's home, and the placing of the same device in the target's private vehicle.

[20] Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v. Minister for Communication et al and Kärtner Landesregierung et al, judgment of 8 April 2014, nyr.

the EU data retention directive of 2006.[21] This ruling, related to one major dimension of the framework for electronic mass surveillance, has been taken into account in the fundamental rights assessments that in their entirety are included as Annex 1 to actual deliverable D2.8. A summary of the six assessments follows below as section 6.3, after section 6.2 that discusses the above-mentioned ruling by the CJEU. The CJEU's ruling also supports the methodology developed for the fundamental rights assessments, as it is a relatively neat and illustrative example of right-based judicial review of legislation for its compatibility with fundamental rights, including the application of the permissible limitations test under Article 52.1 of the Charter of Fundamental Rights of the European Union (CFREU).

The selection of surveillance technologies applied in the terrorism prevention scenario addressed in this deliverable was informed by an assessment of what is known, on the basis of the so-called Edward Snowden revelations and other available sources, of the methods of electronic mass surveillance applied by the National Security Agency of the United States of America. Our scenario represents an adaptation of some of those methods, coupled with two traditional, non-technological surveillance techniques.

The multidimensional assessment by the SURVEILLE consortium of the use of surveillance in the hypothetical terrorism prevention scenario produced striking results. Only the two traditional (non-technological) surveillance methods produced usability and fundamental rights intrusion scores and an assessment of possible ethical risks that would make them *justified*, using the same criteria that were used in deliverable D2.6. Three methods of electronic surveillance are assessed as legally *impermissible,* as they resulted in modest usability scores (between 4 and 5 only), coupled with the highest possible fundamental rights intrusion score (16) and the highest degree of ethical risk (red). Only one of the methods of electronic surveillance – social network analysis – is assessed as *highly suspect* (instead of manifestly impermissible), as it produces high scores both as to usability and fundamental rights intrusion, coupled with intermediate ethical risk. While all other methods of electronic surveillance failed drastically under our fundamental rights assessment, our results suggests that social networking analysis might be used in a manner where the security benefits do justify the intrusion into privacy and data protection rights, provided that due care is taken of providing a proper legal basis for it and subjecting it to a regime of judicial authorization.

These outcomes may be surprising as they result in wide rejection of current methods of electronic mass surveillance on legal and ethical grounds. They are nevertheless supported by the 8 April 2014 ruling of the CJEU, reported below.

[21] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L105, p. 54).

§6.2 The CJEU Ruling on the EU Data Retention Directive

On 8 April 2014, the Court of Justice of the European Union (the CJEU) ruled in Joined cases C-293/12, C-594/12 *Digital Rights Ireland and Seitlinger and Others*[22] that Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC ("Data Retention Directive")[23] is invalid. As the judgment clarifies the status in EU law in respect of the right to privacy and the protection of personal data, also in matters related to surveillance, we have included here a short assessment of the judgment.

The judgment was issued within the preliminary reference procedure under Article 267 Treaty on the Functioning of the European Union (TFEU) in two cases in which *the High Court* (Ireland) and the *Verfassungsgerichtshof* (Austria) had asked the CJEU to examine the validity of the directive in light of Article 7 (the respect for private life and communications), Article 8 (the protection of personal data) and Article 11 (respect for freedom of expression) of the Charter of Fundamental Rights of the European Union (the CFREU or the Charter), while also taking into account Article 52(1) of the CFREU enumerating conditions for the limitations of the rights enshrined in the Charter. The legal effect of the judgment ('preliminary ruling') is binding and final as to the EU law issues, so that the national courts in question can in its light decide the original dispute between the parties.

By its preliminary ruling, the CJEU declared the directive to be invalid, because the EU legislature had "exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter".[24] According to the CJEU, the directive failed to lay down "clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter", as well as entailed "a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary".[25] As the CJEU has not limited the temporal effect of its judgment, the

[22] Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v. Minister for Communication et al and Kärtner Landesregierung et al, judgment of 8 April 2014, nyr.

[23] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L105, p. 54)

[24] Joined cases C-293/12, C-594/12 Digital Rights Ireland and Seitlinger and Others, at paragraph 69.

[25] Joined cases C-293/12, C-594/12 Digital Rights Ireland and Seitlinger and Others, at paragraph 65.

declaration of invalidity takes effect from the data on which the directive entered into force, i.e. on 15 March 2006.

As the judgment is by a Grand Chamber of the Court, an enlarged composition of 15 judges reserved for high-profile cases, the judgment will feature as a precedent which sets out the EU law approach with regard to the manner in which the collection and storage of meta-data produced in the course of electronic communications should be approached in light of the right to privacy and the right to the protection of personal data.

The judgment features as a strong vindication of privacy and data protection as genuine fundamental rights. The erosion of these rights in the fight against terrorism and in respect of increasing surveillance has been a matter of concern in recent years but the judgment now demonstrates that these rights must be taken seriously while countering terrorism and serious crime in general.[26] Even if, at a general level, the objective of preventing and fighting terrorist offences and serious crime can certainly be regarded as a legitimate one, the judgment displays that any interference with the right to privacy and the protection of personal data must be done in accordance with the permissible limitations test and the fundamental rules pertaining to the protection of personal data. In particular, the judgment proves that even highly important aims such as those related to the fight against terrorism cannot justify the adoption of measures which result in forms of interferences going beyond what is strictly necessary and proportionate.

§6.2.1 Fundamental Rights Intrusion Assessment by the CJEU

The April 2014 judgment by the CJEU is a relatively neat and illustrative example of the right-based judicial review of legislation for its compatibility with fundamental rights, including the application of the permissible limitations test under Article 52.1 of the CFREU. After depicting the legal context of the case and the questions referred by the national courts for a preliminary ruling, the reasoning of the CJEU progresses through the following three major questions towards an overall conclusion: Whether the directive falls within the scope of Articles 7, 8 and 11 of the CFREU? Whether the data retention directive constitutes an interference with the right to respect for private life and the protection of personal data? Whether such interferences can be justified under Article 52(1) of the CFREU, providing that "(a)ny limitation on the exercise of the rights and freedoms laid down by the Charter must be provided for by law, respect their essence and, subject to the principle of proportionality, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of

[26] See e.g. Martin Scheinin, Report by the Special Rapporteur on the Promotion and Protection Human Rights and Fundamental Freedoms while Countering Terrorism, A/HRC/13/37, para. 17 (28 December 2009).

general interest recognised by the Union or the need to protect the rights and freedoms of others."

The fundamental rights affected. The CJEU could easily conclude that the obligation on providers of publicly available electronic communications services or of public communications networks to retain the data listed in Article 5 of the directive for the purpose of making them accessible, if necessary, to the competent national authorities raised "questions relating to respect for private life and communications under Article 7 of the Charter, the protection of personal data under Article 8 of the Charter and respect for freedom of expression under Article 11 of the Charter".

However, the Court's only focused on the right to privacy and the protection of personal data because the directive "directly and specifically affects private life" and because the retention of data "constitutes the processing of personal data" and, therefore, "necessarily has to satisfy the data protection requirements arising from that article".[27]

Interference with the rights laid down in Articles 7 and 8 of the Charter. To establish the existence of an interference with privacy and data protection, it largely, if not exclusively, sufficed for the CJEU to note that the retention of data for the purpose of possible access to them by the competent national authorities "derogates from the system of protection of the right to privacy established by Directives 95/46 and 2002/58 with regard to the processing of personal data in the electronic communications sector".[28] Moreover, the CJEU observed with reference to its previous judgment in the cases of *Österreichischer Rundfunk and Others*[29] that an interference with privacy is constituted irrespective of "whether the information on the private lives concerned is sensitive or whether the persons concerned have been inconvenienced in any way".[30] As the directive "provides for the processing of personal data",[31] there was also an interference with the protection of personal data.

Finally, the CJEU quite emphatically underscored that the interference with the rights to privacy and the protection of personal data should be regarded as being "wide-ranging" and "particularly serious". The CJEU added that the fact that "data are retained and subsequently used without the subscriber or registered user being informed is likely to

[27] Joined cases C-293/12, C-594/12 Digital Rights Ireland and Seitlinger and Others, at paragraphs 28 and 29.

[28] Joined cases C-293/12, C-594/12 Digital Rights Ireland and Seitlinger and Others, at paragraph 32.

[29] Cases C-465/00, C-138/01 and C-139/01 Österreichischer Rundfunk and Others EU:C:2003:294, paragraph 75.

[30] Joined cases C-293/12, C-594/12 Digital Rights Ireland and Seitlinger and Others, at paragraph 33.

[31] Joined cases C-293/12, C-594/12 Digital Rights Ireland and Seitlinger and Others, at paragraph 36.

generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance".[32]

Justification of an interference with privacy and data protection. The bulk of the judgment deals with the justification of the interference by data retention with the rights guaranteed by Articles 7 and 8 of the Charter, i.e. whether the directive complies with the permissible limitations test under Article 52(1) of the CFREU. In practice, the CJEU's reasoning largely revolves around the proportionality of the interference whereas other conditions attracted less judicial attention.

The essence of a fundamental right is not subject to restrictions. The CJEU rejected the argument raised by the some of the parties that the directive entails the violation of the essence of the fundamental rights to privacy and data protection. Even if the retention of extensive metadata by the directive does constitute a particularly serious interference with those rights, the CJEU took the view that directive "does not permit the acquisition of knowledge of the content of the electronic communications as such".[33]

Thus, the CJEU's reasoning seems to suggest that the interference came close to the core area of privacy and data protection rights but did not cross that border, thereby alluding to a possible interpretation that only content might pertain to the essence of the fundamental rights at issue. In that regard, the CJEU's view can be even be criticized for being too conventional. After all, the distinction between "content data" and metadata (such as traffic data and location data) is rapidly fading away in modern network environment. A lot of information, including sensitive information, about an individual can be revealed by monitoring the use of communications services through traffic data collection, storage and processing. Hence, the processing of metadata cannot any longer be invariably seen as falling within such "peripheral areas" of privacy and data protection where limitations would always be legitimate and permissible. The more systematic and wide the collection, retention and analysis of metadata becomes, the closer it can be seen as moving towards the core area of privacy and data protection. It cannot be excluded that at least the most massive, systematic forms of collection and analysis of metadata can constitute an intrusion into the core of privacy and data protection.

Legitimate aim. According to the CJEU, it was "apparent" from its previous case law that the material objective of the directive, namely "the fight against international terrorism in order to maintain international peace and security", as well as "the fight against serious crime in order to ensure public security" constituted an objective of general interest within the meaning of Article 52(1) of the CFREU. In addition, the CJEU noted

[32] Joined cases C-293/12, C-594/12 Digital Rights Ireland and Seitlinger and Others, at paragraph 37.

[33] Joined cases C-293/12, C-594/12 Digital Rights Ireland and Seitlinger and Others, at paragraph 39.

that the directive served to protect the rights and freedoms of others as "Article 6 of the Charter lays down the right of any person not only to liberty, but also to security."[34]

The proportionality of the interference. The CJEU began its assessment of the proportionality of the interference by recalling that the acts of the EU institutions "be appropriate for attaining the legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives".[35] The CJEU also noted that its judicial review of the EU legislature's discretion "should be strict" because of "the important role played by the protection of personal data in the light of the fundamental right to respect for private life and the extent and seriousness of the interference with that right caused by Directive 2006/24."[36] In addition, the Court emphasized that even highly important objectives such as the fight against serious crime and terrorism cannot justify measures which lead to forms of interference that go beyond what is "strictly necessary".[37]

Next, the CJEU identified five distinct, yet inter-related defects of the directive that combined to justify the overall conclusion that "the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter". *First*, the directive failed to set any limit on the personal scope of application as it "affects, in a comprehensive manner, all persons using electronic communications services" and, accordingly, "applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime."[38] *Second*, the Directive remained too vague regarding how precisely could the legitimate objective of countering terrorism and serious crime be served by the directive. In particular, the directive failed to restrict the scope of application of a retention in relation "(i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences."[39] *Third*, the directive fell short of limiting appropriately the access of national authorities to the data retained by private companies. In particular, the directive did not made access dependent "on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which

[34] Joined cases C-293/12, C-594/12 Digital Rights Ireland and Seitlinger and Others, at paragraph 42.

[35] Joined cases C-293/12, C-594/12 Digital Rights Ireland and Seitlinger and Others, at paragraph 46.

[36] Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, at paragraph 48.

[37] Joined cases C-293/12, C-594/12 Digital Rights Ireland and Seitlinger and Others, at paragraph 51.

[38] Joined cases C-293/12, C-594/12 Digital Rights Ireland and Seitlinger and Others, paragraph 58.

[39] Joined cases C-293/12, C-594/12 Digital Rights Ireland and Seitlinger and Others, at paragraph 59.

intervenes following a reasoned request of those authorities."[40] *Fourth*, the Directive merely required the data to be retained for a period of at least six months, "without any distinction being made between the categories of data set out in Article 5 of that directive on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned."[41] Fifth and finally, the Directive did not provide for sufficient safeguards relating to the security and protection of data retained by private providers of electronic communications.[42]

In light of all these flaws, the CJEU made the interim conclusion that the directive failed to "lay down clear and precise rules governing the extent of the interference" with the rights affected and, accordingly, "entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary."[43]

§6.2.2 Consequences of the judgment

The immediate effect of the judgment is that the data retention directive has become entirely invalid *ex tunc*, i.e. from the date on which the directive had entered into force. Indeed, it is noteworthy that the CJEU did not limit the temporal effects of the finding of invalidity although it has the competence to do so if overriding considerations of legal certainty so require.

Where the CJEU rules that a directive is invalid, its decision has the legal effect of imposing a *positive obligation* on the EU legislature to take all the necessary measures to remedy that illegality. Indeed, it deserves to be emphasized in this context that while the CJEU may find that EU legislation violates fundamental rights and, accordingly, invalidates such legislation, this judicial power cannot substitute the positive obligation of the EU legislature to provide such legislation that is compatible with the requirements of fundamental rights.

The finding of invalidity of the directive by the CJEU does not, as such, affect the validity of domestic implementing measures of that directive. After all, the CJEU has no competence to rule, in the preliminary ruling procedure that addresses issues of EU law, that a national legal measure is invalid. According to Article 51(1) of the CFREU, however, the EU Charter of Fundamental Rights, including its Articles 7 and 8 on the

[40] Id., § 62.

[41] Id., § 64.

[42] Id., § 66.

[43] Joined cases C-293/12, C-594/12 Digital Rights Ireland and Seitlinger and Others, at paragraph 65.

right to privacy and the protection of personal data, is binding on the Member States “"when they are implementing Union law". As a matter of EU law, the CFREU, as now being interpreted by the CJEU in the present case, should apply whenever the Member States apply their national laws implementing the data retention directive. Furthermore, it is not sufficient for Member State authorities just to disregard their own domestic provisions which are incompatible with the requirements of the right to respect for private life and the protection of personal data under the CFREU, as now interpreted by the CJEU in the present case. The Member States are also under a positive obligation to amend their national implementing legislation, to provide a legislative framework regarding data retention at the level of national law that is compatible with privacy and data protection.

One of the most crucial questions now is to what extent, if any, mandatory data retention can be adequately regulated by EU legislation so that all requirements of the right to respect for private life and the principles regulating the processing of personal data are complied with. It falls beyond the purpose of this analysis to ponder this question in detail. Instead, it suffices here to note that the judgment is not a total knockout by the CJEU of data retention. While the judgment clearly displays that mass surveillance based on vaguely defined provisions is not compatible with the requirements of the right to respect for private life and the protection of personal data under Articles 7 and 8 of the CFREU, the basic undertone of the judgment nonetheless seems to be that some form of mandatory data retention in order to combat serious crime and terrorism might indeed be compatible with the EU Charter of Fundamental Rights. What is more, the CJEU can even be understood as delineating carefully such points that should be taken into account by the EU legislature when curtailing data retention to what is “strictly necessary”. These points can largely be inferred from those observations of the CJEU specifying the flaws of the data retention directive that jointly triggered the outcome that the directive exceeded the limits of what is appropriate and strictly necessary in order to achieve the legitimate objectives. However, as it is beyond the powers of the CJEU to establish the legislative framework required, a positive obligation is now imposed on the EU legislature and, later, the Member States to organize such a legal regime for data retention that appropriately complies with the requirements of the right to respect for private life and the protection of personal data.

§6.3 Summary of the SURVEILLE Fundamental Rights Assessments of the Terrorism Prevention Scenario

The methodology developed in SURVEILLE deliverable D2.6 was used to assess the fundamental rights intrusion resulting from the use of the six surveillance technologies or techniques, as applied in the terrorism prevention scenario. In practice, the assessments focused on the right to the protection of private life (or privacy) and the right to the protection personal data. As the possible intrusion into other fundamental rights, such as freedom of expression or freedom of association, was found to be derivative in nature, resulting from the first-order intrusion into privacy or data

protection rights, the scoring was conducted only in relation to the rights immediately impacted.[44]

As in earlier deliverable D2.6, the fundamental rights intrusion scores 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 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 a fundamental rights or, similarly, low, medium or high level of intrusion into that right. The two scores are then multiplied with each other to give a combined score from 1 to 16 – or 0 where no fundamental rights impact could be identified.[45]

The primary source material used to assign the scores (low/medium/high) was found in existing case law by the European Court of Human Rights (ECtHR), complemented by the case law of the EU Court of Justice (including under the EU Charter of Fundamental Rights) and the United Nations Human Rights Committee acting under the International Covenant on Civil and Political Rights. The scoring is accompanied by detailed reference to this body of case law related to identical, similar or analogous situations. The scoring has been verified collectively by the team of legal experts functioning as the EUI team in SURVEILLE. Where existing case law by the ECtHR and other relevant authorities was absent or ambiguous, the score has been corrected by multiplying it by ¾. A similar reduction of the intrusion score by one fourth (i.e., multiplication by ¾) would be applied if the use of a surveillance method was authorised by a court. In practice, as none of the surveillance methods applied in the scenario had judicial authorization, no such reduction of the score was possible this time.

Where the methodology applied in deliverable D2.6 and subsequently this Paper extracted from deliverable D2.8 has a limitation is that the scenario is presented as jurisdiction-neutral. This constrains the possibility fully to assess whether each fundamental rights intrusion was compatible with the requirement of being "in accordance with the law", which includes an assessment not only of the existence of national legislation but also of its qualitative features, as to whether it provides an

[44] The recent ruling of the CJEU on the invalidity of the Data Retention Directive also supports the limitation of focus on the rights immediately impacted. Although the CJEU acknowledged that the retention of the data might also have an effect on the freedom of expression guaranteed by Article 11 of the CFREU, it examined the validity of the directive in the light of Articles 7 (the right to private life) and 8 of the CFREU (the right to the protection of personal data) only because the retention of data for the purpose of possible access to them by the competent national authorities "directly and specifically affects private life", as well as constituted the processing of personal data within the meaning of Article 8 and, therefore, necessarily has to satisfy the data protection requirements arising from that article. See Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v. Minister for Communication et al and Kärtner Landesregierung et al, judgment of 8 April 2014, nyr., at paragraph 29.

[45] For a discussion of the methodology and its theoretical background, see SURVEILLE deliverable D2.6, section 2.3.3.

adequate basis for restricting a fundamental right. Where a restriction of a fundamental right is found to lack proper legal basis, it will be legally impermissible, irrespective of the weight of the right or the depth of the intrusion, as long as there nevertheless is an identified intrusion without proper legal basis. Even if our scenario is presented as jurisdiction-neutral, we have included in the assessments certain assumptions or conditions concerning the existence and quality of the legal basis available for each surveillance method.

The resulting scores are presented in the below. As can be seen, in four out of six cases the assessments produced identical scores for privacy and data protection, and in three of these the maximum score of 16 under each of the two fundamental rights. No intrusion into data protection rights was identified with the two traditional (non-technological) surveillance techniques, and in these two cases also the resulting score for privacy intrusion was very low (3/4).

Technology or technique	Fundamental right to the protection of personal data				Fundamental right to the protection of privacy			
	Abstract weight	Intrusiv-eness	Reliability of the law	Value	Abstract weight	Intrusiv-eness	Reliability of the law	Value
1. Optical splitter	4	4	1	16	4	4	1	16
2. Phantom viewer	4	4	1	16	4	4	1	16
3. Social network-ing analysis	2	4	1	8	2	4	1	8
4. Opening of baggage	-	-	-	-	1	1	3/4	3/4
5. Covert surveillance team	-	-	-	-	1	1	3/4	3/4
6. Finspy	4	4	1	16	4	4	1	16

A brief account of the justification for these scores follows below. For the more detailed complete assessments and for the sources used to verify each step of the assessments, reference is made to Annex 1 of SURVEILLE deliverable D2.8.

§6.3.1 Optical splitter (paragraph 3 of the scenario)

The Minister, a member of the executive, has approved an interception warrant which allows the signals intelligence agency to intercept all communications that flow through a specific submarine cable between country Z and another EU Member State. This form of electronic mass surveillance falls under the 'jurisdiction' of state Z, as it is conducted by its authorities and most likely on the soil of country Z, and as it affects the fundamental rights of individuals present in the country.

Already mere interception by the authorities of the communications, irrespective of their subsequent use, amounts to an interference with both the right to privacy and the right to the protection of personal data of affected individuals. Although the prevention of terrorism is a legitimate objective for restrictions upon privacy and data protection rights, the surveillance method in question does not meet the other requirements of a permissible limitation. The weight of both fundamental rights is assessed as high (4) in the context at hand, because the intrusion affects the right of individuals to decide what information to share with whom, coming close to the core of privacy, and as the interception unavoidably includes also all sensitive personal information. Also the level of intrusion is assessed as high (4) in respect of both rights, as the measure is massive and systematic and as the vast majority of intercepted data concerns persons over whom there is no basis whatsoever for suspicion of terrorism and hence no relation with the as such legitimate objective of the surveillance.

The existing case-law by the ECtHR and other authoritative bodies, including the judgment of the CJEU on the invalidity of the data protection directive, provides a reliable basis for these assessments (1). There was no judicial authorization for the measure (1).

The resulting intrusion score is 16 (the maximum) for both privacy and data protection, indicating that even the very highest level of security benefit would not justify the surveillance method. In addition, on the basis of what is said in the scenario, it appears that the domestic law of country Z provides an insufficient legal basis for the measure which therefore would be legally impermissible also on this ground alone.

§6.3.2 Phantom viewer (paragraph 8)

Officials of the signals intelligence agency have made a list of ‘selectors’ on the basis of a interception warrant certificate, to examine the communications obtained in the preceding phase. The selectors allow sorting out information concerning specific individuals, including their passwords and other sensitive material. This form of examination, use and storage of information amounts to an interference in both privacy and data protection rights.

Although the prevention of terrorism is a legitimate objective for restrictions upon privacy and data protection rights, the surveillance method in question does not meet the other requirements of a permissible limitation. On the basis of the scenario it appears that the domestic law of country Z does not meet the quality of the law test to provide a proper legal basis for the measure. The weight of both fundamental rights is assessed as high (4) in the context at hand, because the intrusion affects the right of individuals to decide what information to share with whom, coming close to the core of privacy, and as the interception unavoidably includes also all sensitive personal information. Also the level of intrusion is assessed as high (4) in respect of both rights, as the measure is massive and systematic and there will be a high degree of third-party intrusion, as the vast majority of the data processed by the use of selectors concerns persons over whom there is no basis whatsoever for suspicion of terrorism and hence

no relation with the as such legitimate objective of the surveillance. The intrusion lacks proportionality in relation to the benefit obtained towards the legitimate aim of preventing terrorism.

The existing case-law by the ECtHR and other authoritative bodies, including the judgment of the CJEU on the invalidity of the data protection directive, provides a reliable basis for these assessments (1). There was no judicial authorization for the measure (1).

The resulting intrusion score is 16 (the maximum) for both privacy and data protection, indicating that even the very highest level of security benefit would not justify the surveillance method. In addition, RIPA was assessed to provide an insufficient legal basis for the measure, which therefore is legally impermissible also on this ground alone.

§6.3.3 Social networking analysis (paragraph 8)

The data obtained through the use of 'selectors' in the previous phase is subjected to further analysis to produce a 'social graph' of persons of interest and their connections. A vast majority of the resulting data on social interaction is without relevance for intelligence or terrorism prevention. While the measure will in many cases result in an interference with freedom of association and freedom of expression, our analysis focuses on its first-order intrusion into privacy and data protection rights, amounting to an interference.

Although the prevention of terrorism is a legitimate objective for restrictions upon privacy and data protection rights, the surveillance method in question does not meet the other requirements of a permissible limitation. On the basis of the scenario it appears that the domestic law of country Z does not meet the quality of the law test to provide a proper legal basis for the measure. The weight of both fundamental rights is assessed as medium (2) in the context at hand, as the measure entails a clear intrusion but is less all-encompassing than the methods applied in the two earlier stages. Nevertheless, the level of intrusion is assessed as high (4) in respect of both rights, as the measure is massive and systematic and is open to abuse and arbitrariness.

The existing case-law by the ECtHR and other authoritative bodies, including the judgment of the CJEU on the invalidity of the data protection directive, provides a reliable basis for these assessments (1). There was no judicial authorization for the measure (1).

The resulting total scores (8 for privacy and 8 for data protection) demonstrate serious interference in fundamental rights that can only be justified if the security benefit (represented by the usability score) was at or close to its maximum value (9 or 10). However, that would be the case only if proper legal basis existed for the intrusion. As this was not the case, the social networking analysis fails the permissible limitations test already because its regulation does not meet the "in accordance with the law" requirement.

§6.3.4 Opening of baggage (paragraph 9)

At this stage the scenario moves to traditional (non-technological) surveillance of an individual target, identified through the preceding measures of electronic surveillance. As the person is arriving in country Z by airplane, his checked-in suitcase is secretly opened in order to detect explosives or other prohibited items. This measure constitutes an interference with the target's right to privacy but not his data protection rights. The covert opening of the suitcase of an identified target is assessed as being based on the legitimate aim of preventing terrorism, as proportionate towards that aim and as being in accordance with the law.

The weight to the right to privacy in the given context is assessed as low (1), as it is well regulated and well known that luggage transported by air is subject to security regulations and screening as to the presence of prohibited items and substances. Also the intensity of the interference is assessed as low (1), because the target was subjected to the measure on the basis of individual suspicion that he was trying to transport prohibited items and the search was not abused for other purposes (such as the examination of diaries or computer hard disks). There was no judicial authorization for the measure (1). As there is, on the basis of existing case-law, some doubt whether the measure even reached the level of an 'interference', the score (1x1x1) is reduced by one quarter and comes out as ¾. This represents the lowest possible degree of privacy intrusion, suggesting that even a fairly modest security benefit will suffice as its justification.

§6.3.5 Covert surveillance team (paragraph 11)

Another traditional (non-technological) surveillance method applied in the scenario is the visual observance of the same target as in the preceding phase, by a surveillance team while he is in a public place, namely an internet café. Again, this measure is assessed as constituting an interference with the target's right to privacy but not his data protection rights. The covert visual surveillance is assessed as being based on the legitimate aim of preventing terrorism, as proportionate towards that aim and as being "in accordance with the law", as the domestic law of EU Member States routinely appears to provide a proper legal basis for this type of visual surveillance of a specific target.

The weight of the right to privacy in the given context is assessed as low (1), as the surveillance takes place in public space where the target is able to regulate his own conduct to take into account the possibility of being seen or overheard. Also the intensity of the interference is assessed as low (1), because the target was subjected to the measure on the basis of individual suspicion. Hence, the measure was assessed as proportionate and necessary towards the legitimate aim of preventing terrorism. There was no judicial authorization for the measure (1). As there is, on the basis of existing case-law, some doubt whether the measure even reached the level of an 'interference', the score (1x1x1) is reduced by one quarter and comes out as ¾. This represents the

lowest possible degree of privacy intrusion, suggesting that even a fairly modest security benefit will suffice as its justification.

§6.3.6 Finspy equipment (paragraph 12)

The last surveillance method used in the scenario is the installation of Finspy equipment on the computers the target might use when visiting an internet café, remotely to follow all forms of communication including Skype, chat, e-mail, contact lists and internet browsing. This type of surveillance is assessed as an interference both in the privacy rights and data protection rights of the target, as well as anyone he is communicating with. As the target has been identified as a person of interest in a terrorism prevention scheme, there is a legitimate aim behind it. Whether the interference was "in accordance with the law" as required by Article 8 of the ECHR, depends on the level of precision provided in the warrant but we are prepared to assume that the domestic law of EU Member State Z would contain the legal provisions for a properly crafted warrant. There would, however, be no judicial authorization under the RIPA, for which reason the below scores will not be mitigated on that ground.

The weight of the privacy and data protection rights of the target are assessed as high (4) in the situation at hand. The surveillance interferes with his liberty right of being able to decide what information to share and with whom and is therefore considered to fall close to the core of the right to private life. Finspy catches sensitive personal data of both the target and his interlocutors. Also the intensity of the intrusion is assessed as high (4), as it catches all types of communication by the target and unavoidably results in the indiscriminate subjugation of the target's interlocutors to the same intrusive form of surveillance. In the assessment we also discuss factors that could make the surveillance more targeted and transform the level of intrusion from high to moderate. That is, however, not the case here and therefore the outcome is the maximum score of 16. As the assessment is based on clear case-law, the reliability of the assessment is high (1) and the score need not be mitigated. The resulting intrusion score is 16 for both privacy and data protection, indicating that even the very highest level of security benefit would not justify the surveillance method under European and international law, even if a its use was prescribed in domestic law.

§7 Summary

A key task of SURVEILLE deliverable D2.8 has been continuing the assessment of surveillance technologies according to the framework developed in SURVEILLE deliverable D2.6. While some of the modes of presentation in the matrix have been adjusted, it contains the same combination of ethical, legal and technological assessment, and like D2.6, it attempts to focus this analysis on realistic uses of these technologies by investigators. D2.6 was focused on a serious crime investigation, where suspected gun and drug runners were subjected to a range of different traditional surveillance techniques including chemical explosives detectors, CCTV and drones, and

much more intrusive methods such as bugging and phone tapping. There was no real correlation between technologies that scored well for usability and those that scored well ethically or with regard to their impact on fundamental rights. There was also some disagreement between the permissibility of the most intrusive technologies between the ethical and fundamental rights assessment.

In D2.8 we have considered the case of mass Internet monitoring systems that are publicly justified on the basis of their counter-terrorism application, and we bring our analysis to bear on their use for a counter-terrorism investigation – exactly the sort of case where justification of its use ought to be strongest. Various kinds of Internet monitoring techniques are applied side by side with more traditional surveillance techniques. We find most of the Internet monitoring applications both ethically and legally impermissible, assessing them poorly in comparison with traditional, non-technology based surveillance methods. Furthermore, the Internet monitoring techniques compare poorly with the traditional techniques also in terms of usability. The conclusions of D2.8 are much more clear cut than those of D2.6: Internet monitoring techniques, with the exception of targeted social networking analysis, represent an unacceptable interference with fundamental rights to privacy and data protection, the deepest ethical risks of chill and damage to trust, intrusion and discrimination, while also violating moral norms of proportionality of methods and consent of the policed. Meanwhile these high moral and legal costs reflect a mostly middling to poor usability benefit, performing worse with regard to cost, efficiency and privacy-by-design than lower tech alternatives. The case for a mass Internet monitoring system is found wanting.

Annex: Alternative Matrix of Surveillance Technologies

Matrix								
TECHNOLOGY AND USE	USABILITY	FUNDAMENTAL 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) / Moral risk of Intrusion	Consent	Moral risk of discrimination	Moral risk of damage to trust and chilling effect	Ethical proportionality
1. Cable Splitting Fiber optic backbone	5		4x4x1	4x4x1				
2. Phantom viewer	5		4x4x1	4x4x1				
3. Social networking analysis	8		2x4x1	2x4x1				
4. Opening baggage	8			1x1x¾				
5. Covert surveillance team	6			1x1x¾				
6. Finspy	4		4x4x1	4x4x1				

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. **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.