SYnergy of integrated Sensors and Technologies for urban sEcured environMent

D10.7
GUIDELINES FOR DEPLOYMENT OF THE SYSTEM TECHNOLOGIES

15 March 2021 **V3.0**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 787128

Project title	SYnergy of integrated Sensors and Technologies for urban sEcured environment
Project acronym	SYSTEM
Project number	787128
Start date of the project	1st September, 2018
Duration	36 months
Topic	SEC-10-FCT-2017. Integration of detection capabilities and data fusion with utility providers' network

Deliverable number	D10.7
Deliverable title	Guidelines for deployment of the SYSTEM technologies
Leading partner	VUB
Partners contributing	//
WP of reference	WP10
Title of the WP of reference	LEGAL AND ETHICS MANAGEMENT
Task of reference	T10.1 T10.3
Title of the task of reference	BASELINE KNOWLEDGE AND COMPLIANCE WITH ETHICAL, REGULATORY AND SOCIAL ACCEPTANCE CONDITIONS AND AREAS OF CONCERN FOR SYSTEM LEGAL AND ETHICS MANAGEMENT
Deliverable type	Report
Dissemination level	PUBLIC
Due date	M42 - February 2022

Keywords	Tests; compliance; ethics; legal conditions; questionnaire
Abstract	The report consolidates the lessons learnt throughout the project's WP10 and offers a set of tentative guidelines for the deployment of the SYSTEM technologies, from ethical and legal points of view.

Editor	AND Consulting Group (AND Consult, subcontractor of VUB), Eugenio Mantovani (VUB)
Contributors	Sergy Vazquez Maymir (VUB), AND Consult
Reviewers	Lorenzo Di Matteo (FORMIT)
Submission date of the draft to reviewers	Not required
Submission date of the	//

draft to the SAB (if required)	

Register of document versions

Partner acronym	Version number	Date	Suggested relevant changes	Notes
AND Consult /VUB	V1.0	15/11/2021	ToC and Draft intro	//
AND Consult /VUB	V1.1	30/11/2021	Validation seminar to be hosted at CPDP 2022 (January)	//
AND Consult	V1.2	20/12/2022	First draft	Writing of the core text of the document
VUB/ AND Consult	V1.3	5/01/2022	Comments and revision	CDPD 2022 seminar cancelled due to COVID_19 and postponed to May 2022
VUB / AND Consult	V1.3	30/01/2022	New comments from recent tests	Participation and involvement of 'passer-by'
VUB	V1.4	01/03/2022	Final draft	Draft to VUB for submission
FORMIT	V2.0	13/03/2022	//	Review version
FORMIT	V3.0	15/03/2022	//	Final version

Every information is updated to the date of issue of this document

This document is composed by 30 pages

Table of Contents

List of acronyms and abbreviations

CA	Consortium Agreement
CCTV	Closed-Circuit Television
DoA	Description of Action
DPIA	Data Protection Impact Assessment
EC	European Commission *or* Electrical Conductivity
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
ES	Exploitation Strategy
GA	Grant Agreement
GDPR	General Data Protection Regulation
GPS	Global Positioning System
LC/MS	Liquid Chromatography/Mass Spectrometry
LEA	Law Enforcement Agency
NGO	Non-Governamental Organisation
PIN	Privacy Impact Notice
SME	Small and Medium Enterprise
UAV	Unmanned Aerial Vehicle
WP	Work Package

EXECUTIVE SUMMARY

The aim of this deliverable is to consolidate the lessons learnt about SYSTEM's legal and ethical impacts with a view to offer a set of tentative guidelines for the deployment of the SYSTEM technologies.

The guidelines delve into the main legal and ethical issues likely to be mobilised when a research project or policy decision leads to the integration of SYSTEM sensors and technologies in a European city.

This is a tentative set of guidelines, addressed primarily to researchers and policymakers, which can be used as a basis for discussion and deliberation. The first guideline delves into trust, transparency, oversight, and information. Another guideline invites policymakers to debate, before deployment, the necessity, the proportionality, as well as to ensure accuracy and explainability of SYSTEM-like surveillance systems. SYSTEM does not infringe on the privacy of homes, nor does it collect any personal data. However, the deployment of these technologies should, in any case, consider the chilling effect of surveillance on private life and assess, for instance by means of a DPIA, whether personal data is or not actually collected and processed. Finally, policymakers are invited to recognise that surveillance measures can have social and psychological impacts.

INTRODUCTION

This document is part of the project's Work Package (WP) 10, the WP dedicated to identifying and mitigating the non-technological, viz. legal, social or ethical risks raised or emerging during SYSTEM's project activities. The deliverable consolidates the lessons learnt about the project's and SYSTEM technology's legal and ethical impacts with a view to offering a set of tentative guidelines for the deployment of the SYSTEM technologies. The guidelines delve into the main legal and ethical issues likely to be mobilised when a research project or policy decision leads to the integration of SYSTEM sensors and technologies in a European city.

The guidelines discussed in this document, originally, were planned to be discussed in a dedicated one-day workshop. The validation workshop, scheduled to be hosted at a conference (Computers Privacy and Data Protection conference) in January 2022, had to be cancelled due to the COVID-19 pandemic and re-scheduled for the edition of the same conference postponed to May 2022.

The guidelines take stock of the legal and ethical risks and impacts that have emerged during the three (ethical and legal) risk reviews that have accompanied tests in both controlled and controlled environments throughout the duration of the project. As that analysis shows, SYSTEM does not collect personal data. Data collected from sensors in the sewage network include measurements of the interaction of spilled compounds with sensors in the wastewater environment, flow data, data about pH and Electrical conductivity (EC), etc., which can in no way identify a natural person. The use of sensors installed on drones or solid waste trucks does not pose any concern from a privacy or personal data protection perspective either. As for the information to the public, partners have informed, and obtained the authorisation from local authorities to carry out the tests and, e.g., cordon off the streets, enter the manholes. As tests are carried out in the city, partners were prepared to answer questions posed by random citizens walking by the research sites (D10.5).

Against this background, this report presents a series of guidelines addressed to policymakers or research sponsors who are considering the deployment or setting up further research activities leveraging on the capacities and possibilities developed by the SYSTEM project consortium.

STRUCTURE OF THIS DELIVERABLE

The deliverable is organised around five broad areas: trust and governance, justice and fairness, necessity and reliability, deviations, privacy and personal data protection, and social issues. A table in Annex I Table of guidelinessummarises the guidelines.

1. MAIN ELEMENTS OF THIS DELIVERABLE

1.1. INPUT FROM OTHER WPS AND RELATION WITH OTHER SYSTEM DELIVERABLES

The report benefits from inputs coming from Task 10.1 "Baseline Knowledge and Compliance with Ethical, Regulatory and Social Acceptance Conditions and Areas of Concern for System" and Task 10.3 "Legal and Ethics Management", as well as from the main findings of D10.5 "Third Risk Review Report".

1.2. APPLICABILITY

The deliverable is applicable among the Consortium from its first draft and as a final version from its date of submission at the end of the SYSTEM project, without prejudice of successive eventual updates.

1.3. REFERENCE DOCUMENTS

In order to set a framework in a matter of a conflict between the Project Operational and Management Plan (D12.1) and other documents such as the Description of Actions (DoA) or the Grant Agreement, the following hierarchy will be applied:

1. Grant Agreement (GA);
2. Consortium Agreement (CA);
3. The Project Operational and Management Plan (D12.1).

The hierarchy related to the documents above implies that the latter document needs to be consistent with the former. In case of issues, this hierarchy of documents is mandatory.

1.4. PURPOSE OF THE DOCUMENT

The main aim of the report is to present a series of guidelines addressed to policymakers or research sponsors who are considering the deployment or setting up further research activities leveraging on the capacities and possibilities developed by the SYSTEM project consortium.

1.5. STRUCTURE OF THE DOCUMENT

The document is structured in the following way:

2. **Chapter 2** details the **"**Guidelines on trust and transparency**";**
3. **Chapter 3** defines the **"**Guidelines on necessity and reliability**";**
4. **Chapter 4** provides the **"**Guidelines on how to navigate deviations**";**
5. **Chapter 5** illustrates the **"**Guidelines on privacy and data protection /fundamental rights**";**
6. **Chapter 6** describes the **"**Guidelines on social issues**";**
7. **Chapter 7** provides an overview of the main elements of the report in form of "Conclusions**".**

2. GUIDELINES ON TRUST AND TRANSPARENCY

Throughout the project and amongst partners there has been a divergence about the approach to building trust in SYSTEM technology.

Trust is important to the deployment of any surveillance system: the stabilisation of certain types of security technologies, e.g., cameras, is both determined by and at the same influences the level of trust between citizens and Law enforcement agencies (LEAs) in that society. As Conley and colleagues nicely put it, "[w]hen law enforcement fails to fully engage with community members about the impact of surveillance—or, worse, entirely skirts the democratic process by acquiring and deploying surveillance technology without public discussion at all—it erodes trust even further, making it even harder for law enforcement officers to work with the community to solve crimes and protect public safety."[1] Trust, in democratic constitutional systems, speaks of relationships between the individual citizens and the institutions that are responsible for implementing the surveillance. For law enforcement officers to 'work with the community to solve crimes and protect public safety', it is important that institutions (that are responsible for implementing surveillance measures) communicate effectively with the public. Public concerns about planned programmes and the security issues they aim to tackle must be expeditiously identified, acknowledged, and addressed. Leaving such concerns unaddressed can be risky. When a surveillance program is discovered by accident or later (after it is operational), that trust, that key element for law enforcement officers to 'work with the community to solve crimes and protect public safety', is undermined. Consequently, trust in state institutions, in general, is also eroded.

Whilst trust has value for law enforcement purposes, it helps LEAs to solve crimes and protect public safety, it is not easy to communicate about programmes that involve new or unfamiliar technologies: it is not easy to explain, for instance, that as multi-sensor surveillance technologies for detection of precursors for synthetic drugs and home-made explosives is being tested; equally challenging may the task of communicating the necessity for society to tackle threats that may be less well-understood, for instance, stemming the use of laboratories at home or in apartments for development of illegal drugs or explosives.

[1] Conley, C., Cagle, M., Bibring, P., Farris, J., Lye, L., Ebadolahi, M., & Ozer, N. (2016). Making Smart Decisions about Surveillance: A Guide for Community Transparency, Accountability & Oversight. Retrieved from American Civil Liberties Union of California website: www.aclunc.org/smartaboutsurveillance, p. 6.

In the context of SYSTEM, while the importance of creating and building trust is acknowledged, most LEAs partners advocated an approach to trust based on the idea of working responsibly with the technology but maintaining a high degree of secrecy about its nature, scope, and deployment (the secrecy approach). They oppose a more open approach, suggested by other not-LEA partners, built around means of openly communicating with stakeholders about the surveillance technology and programme that is intended to be implemented (the open communication approach).

The lesson learnt from the project is that there are good reasons to mitigate the secrecy approach. First, an advantage of the secrecy approach is that it conceals important and potentially sensitive details about the technology – what it does, how it is used, who it targets, etc. – from the people that you hope to use it to catch. If the adversaries know how you are going to identify them, they will change their approach. Applied in SYSTEM, this approach is viable for investigation; however, it may be problematic if SYSTEM is to be used to deliver viable courtroom evidence (something actually excluded from SYSTEM's research purpose). If sewage monitoring is primarily an investigation or 'diagnostic tool', to be used in operational activity, the interest in secrecy of the measure would be compromised for future investigation, because the sewage monitoring methods are described in the criminal file and thus available to the defendants.[2] This means that when sewage monitoring is not used as evidence, as in SYSTEM, but as a basis for further investigation measures only (e.g., a house search to obtain physical evidence), the need to communicate about the deployment of the technology is less constraining. On the other hand, secrecy and the use of SYSTEM-like technology to gather evidence, discussed in court, seemingly cannot work together. As SYSTEM is used as a 'diagnostic tool', secrecy could be justified, but could not be complete either. There remains, indeed, the need for oversight and control that some institutions must exercise, otherwise, it would not be possible to verify whether an operation of the sewage monitoring has been legitimate. Oversight would be restricted to some institutions, which are not open, but public. In practice, oversight means that absolute secrecy about the kinds of technologies SYSTEM uses is impossible. Complete secrecy, while understandable from an investigation point of view, may also not be desirable, on account of the 'bad press' received by 'smart city' programs relating to or encroaching on security and surveillance. "The latest phase is marked by scattered, local-level resistance by residents to smart-city programs in big cities like Toronto and New York to small

[2] Škorvánek, I., Koops, B.-J., & Timan, T. (2019)., Surveillance, Criminal Procedure, and Regulatory Connection: The Case of Sewage Monitoring (SSRN Scholarly Paper No. ID 3377466), p. 29

towns such as Ross, California — near San Francisco — with less than 2,500 residents. […] Other cities have banned specific technologies such as facial recognition software, amid doubts over its accuracy or concerns over cities stealthily collecting such data on their citizens through video surveillance."[3] Sensor technologies have sparked backlashes across the world from San Diego (below) to Hong Kong.[4] When the city of San Diego decided to attach 'Shotspotter' microphones to the traffic lights, …" the city faced demands for public hearings and greater transparency."[5] The importance of trust in this area is underlined by the institution of a 'Smart City Index 2019', which ranks smart cities worldwide on a number of factors including their attitudes to the use of personal data, facial recognition and overall trust in local authorities (Wray, 2019).

The 'bad press', the need for oversight, the limitation of using some surveillance devices as investigative tools only, suggests that the best course of action would be to mitigate the secrecy approach accepting from the outset of a project or a programme, 'some level' or degree of transparency. This mixed approach is recommended by Škorvánek and colleagues: "Instead of intending to keep the possibilities of sewage monitoring secret for as long as possible, so as not to make offenders aware of this new investigation tool, it might therefore be a wiser strategy for LEAs to anticipate that transparency is needed sooner rather than later, and therefore to proactively develop a policy on what can be publicly disclosed on the operation of the system and which operational details must really be kept secret.[6]

Based on the foregoing, the approach that SYSTEM recommended is "to anticipate that transparency is needed sooner rather than later, and therefore to proactively develop a policy on what can be publicly disclosed on the operation of the system and which operational details must really be kept secret." In concrete, this means communication between LEA stakeholders and municipalities and specifically, elected policymaker representatives. The involvement of stakeholders such as elected representatives is important to design the best, given the circumstances of each case, approach to informing the public about the technology and its use. The

[3] Knowledge@Wharton. (2019, September 24). What's Fueling the Smart City Backlash? Retrieved from https://knowledge.wharton.upenn.edu/article/whats-behind-backlash-smart-cities/

[4] Fussell, S. (2019, August 30). Why Hong Kongers Are Toppling Lampposts. Retrieved from The Atlantic website: https://www.theatlantic.com/technology/archive/2019/08/why-hong-kong-protesters-are-cutting-down-lampposts/597145/

[5] Conley, C. (2017). Making Smart Decisions about Smart Cities. Retrieved from American Civil Liberties Union of Northern California website: https://www.aclunc.org/publications/making-smart-decisions-about-smart-cities, p. 5.

[6] Škorvánek, I., Koops, B.-J., & Timan, T. (2019)., op.cit., p.34.

involvement of the public, local authorities are also intended to ensure that, if certain information must remain secret, this secrecy can be explained in terms of *genuine* security requirements and be agreed upon. In this way, legitimate security requirements and needs for secrecy are respected, while oversight and accountability, on one hand, and democratic participation and awareness, on the other, can be ensured.

2.1. GUIDELINES ON OVERSIGHT AND ACCOUNTABILITY

To achieve an acceptable level of oversight and accountability it is, firstly, necessary to comply with whatever existing laws, regulations, standards, or codes of conduct apply in the given context. Secondly, public authorities involved or informed about plans for the deployment of surveillance measures, such as SYSTEM, may want to ask a series of questions[7]:

- When is surveillance permitted or prohibited?
- What legal or internal process is required to use surveillance?
- How are officers trained before they conduct surveillance?

- How are operators supervised?
- How will misuses of the technology be identified?
- What legally enforceable sanctions exist to deter misuse and abuse of this technology?
- How will the community continue to be informed about the surveillance program?
- How will local officials and the public re-evaluate the decision to engage in surveillance or the existing policies and safeguards?

- Are you only collecting necessary data?
- How will surveillance data be secured?
- Under what circumstances can collected data be accessed or used?
- What limits exist on sharing data with outside entities?
- Does retaining data help accomplish the purpose for which the technology was acquired?

2.2. GUIDELINES ON CITIZEN PARTICIPATION AND PUBLIC AWARENESS

[7] Based on the ACLU's 'Surveillance Use Policy' template. Issues to be addressed include (Conley et al., 2016, op.cit., pp. 17–23).

Oversight and accountability may not be enough. Public authorities may consider that the development or the adoption of a given system requires informing citizens and avoiding the politically disastrous consequences that occur when citizens find out *at a later date* that a surveillance system has been deployed without them knowing about it. There is no best way to engage with the public. SYSTEM legal and ethical analysis commended a proactive approach to inform the public about the tests, in the appropriate form. "In the appropriate form" means that it was up to partner LEAs and the public local authority to decide to what information about tests or demonstrations should be provided to the public. One of the simplest and most effective approaches was by 'giving notice'. According to Conley et al., "the public should be given effective notice that surveillance is being considered". According to this orientation, modern sensor-based surveillance measures create an *asymmetry* in informational privacy, whereby citizens lack knowledge about whether information collection activities are undergoing, about the consequences of such gathering, or of the potential of data crossing and mining from other data sets.[8] To mend this asymmetry, a solution would be to "require Privacy Impact Notices (PINs) before allowing the construction of the deployment of large projects (public or private) that risk having a significant impact on personal information privacy or on privacy in public."[9] The notion of using Privacy Impact Notices to inform citizens about surveillance measures is grounded in the argument, which emanates from legal doctrine in the United States, that today's mass surveillance is "nothing less than a form of pollution of the public sphere".[10] Conceiving mass surveillance as a type of pollution, this scholar underlines the need to start a more informed debate by creating more informed citizens. [11] Like in environmental cases, a Privacy Impact assessment team, would be required to investigate whether any technology *potentially* capable of persistently infringing on some aspects of privacy poses risks, describe them, verify if designers have built mitigation strategies, and deliberate whether a privacy impact notice is necessary, whether the partial notice or full disclosure notice.

[8] Conley, C., Cagle, M., Bibring, P., Farris, J., Lye, L., Ebadolahi, M., & Ozer, N. (2016). Making Smart Decisions about Surveillance: A Guide for Community Transparency, Accountability & Oversight. Retrieved from American Civil Liberties Union of California website: www.aclunc.org/smartaboutsurveillance, p. 12.

[9] Froomkin, A. Michael. "Privacy Impact Notices to address the privacy pollution of mass surveillance." In Timan, Tjerk, Bryce Clayton Newell, and Bert-Jaap Koops, eds. *Privacy in public space: Conceptual and regulatory challenges*. Edward Elgar Publishing, 2017, p.195.

[10] ibid., p.185.

[11] Ibid. p.209.

The privacy notice, thus described, would mean 'notice and consent.' While effective and appropriate in most applications concerning personal data protection, the notice and consent rule is significantly weakened within smart city technologies. Rather than passive tick off exercise, privacy notice, when necessary, should instead lead to proactively engaging the people affected by a surveillance intervention. This means holding public hearings to discuss the smart tech or forming citizen working groups to evaluate new proposals.

It is important to underline that privacy notices can be recommended, but the decision of whether not to adopt them should be taken by LEA and public authority. Should LEAs and public authorities decide to do so, privacy notices should become, not notice and consent, but a line item in a public meeting agenda. This means involving community groups and local media to increase public awareness early in the process and engage the entire community with the issue. When is the privacy notice approach commended? In SYSTEM, the relative merits of the secrecy approach vis-à-vis more open approaches reflect the experimental nature of the research project: the research activities have been in fact centred on testing the technological abilities of sensors and data collection capacities, thus is no way, directly or indirectly, interfering, let alone gathering information, about citizens. In the absence of any impacts on citizens, oversight and accountability were emphasised, while information to the public was reduced to informing citizens on the days of testing via posters or verbal communication (see D10.5 Third Risk Review).

3. GUIDELINES ON NECESSITY AND RELIABILITY

The principle of necessity requires that there be a clear demonstration of why technology like SYSTEM is required. The reliability of any surveillance system is a critical concern. It must be ensured a general knowledge of how the system works.

3.1. NECESSITY

The principle of necessity requires that there be a clear demonstration of why technology like SYSTEM is required. In broad terms, this can be achieved by explaining the severity of the problem of clandestine laboratories for drugs and explosives. Following up on information provided in the SYSTEM DoA:" Rob Wainwright, Europol Director, said "Illicit drug production and trafficking remains one of the largest and most innovative criminal markets in Europe. As it grows more

complex and becomes entwined with other forms of crime, and even terrorism, it represents a key threat to the internal security of the EU". Globalisation and technology innovation is accelerating the rate of change in the drug market: the availability of drug precursors and online marketplaces on the Darknet are creating a new opportunity for production and platforms of access to the drug markets. (SYSTEM DoA, Part B, p. 7)."

But the challenge is to be able to convey this reasoning to the people who are to be affected by the technologies. At a minimum, LEAs and public authorities should be able to communicate to the people who are affected by them, for instance, some city areas or the whole city, the reasoning behind the development of the technology *and* with what authority SYSTEM is deployed. LEAs and city authorities should be ready to offer these basic explanations, regardless of whether secrecy and investigative considerations advise against making the system immediately public. Regardless, LEAs and city authorities should be ready to justify the surveillance intervention.

From a legal point of view, the case-law of the European Court of Human Rights accepts that in general, any surveillance systems are capable of engaging individual rights under Article 8 ECHR, the right to private and family life.

In the Uzun v. Germany judgement of 2 September 2010, the applicant, suspect in bomb attacks by a left-wing extremist movement, complained that his surveillance via GPS had violated his right to respect for private[12] life. However, the Court noted, it had pursued a valid aim, given that the investigation had concerned very serious crimes: the applicant's surveillance by GPS had thus been necessary for a democratic society. The ECtHR recognized that the interest of the state in protecting its national security, balanced against the seriousness of the interference with the applicant's right to respect for his private life.

The case of Peck v. the UK concerned the disclosure of footage filmed in a street by a closed-circuit television (CCTV) camera installed by the local council, showing the applicant trying to take his life. The Court found that the disclosure of CCTV footage related to an attempted suicide was not proportionate given that the objective of prevention could have been achieved through more proportionate means and options. The court clarified that: "The monitoring of the actions of an individual in a public place by the use of photographic equipment which does not record the visual

[12] ECtHR, *Uzun v. Germany*, application no. 35623/05, judgment of 2 September 2010 ("*Uzun v. Germany*").

data does not, as such, give rise to an interference with the individual's private life […] On the other hand, the recording of the data and the systematic or permanent nature of the record may give rise to such considerations."[13]

The P.G. *and J.H. v. the United Kingdom case*[14] concerned the installation of the covert listening device on private property, use of the covert listening device in a police station, and acquisition by police of information relating to the use of a private telephone. Also in those cases, which concerned the permanent recording of the voices of P.G. and J.H., the court clarified that "Private-life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain. It is for this reason that files gathered by security services on a particular individual fall within the scope of Article 8, even where the information has not been gathered by any intrusive or covert method. "

In conclusion, the European court of law accepts that in general, any surveillance systems are capable of engaging individual rights under Article 8 ECHR, i.e., a right to private and family life. However, this does not mean that such 'engagements' can automatically be equated to violations of Article 8. As the case law review indicates, determining what is "proportionate" will depend on a variety of factors:

- The nature of the measure taken (its reach, whether it is general or absolute, its adverse consequences, the scope for abuse of the measure),
- whether the state concerned could have taken other measures or implemented them in a less drastic way,
- any status of the persons involved which legitimately renders their rights subject to greater limitation (e.g., prisoners)
- whether there are any safeguards which can compensate for the infringement of rights which a measure can create.[15]

3.2. RELIABILITY

[13] ECtHR, *Peck v United Kingdom,* (2003) 36 EHRR 41

[14] Case of PJ & H v United Kingdom (Application Number 0004478/98 2001)

[15] See I. Cameron, National Security and The European Convention on Human Rights, The Hague/London/Boston, Kluwer Law International, 2000, (479p.), 97-101 and M. Delmas-Marty, The European Convention for the Protection of Human Rights, Dordrecht, 1992, 71, As quoted in P.de Hert, op.cit., p.80.

The reliability of any surveillance system is a critical concern. It must be ensured a general knowledge of how the system works. At its basic, when a component part of the SYSTEM triggers an alert or alarm, there is a good reason. This requires asking a series of simple questions:

I. What combination of data or circumstances triggers the alarm?

II. Does the alarm initiate a procedure with significant consequences for the targeted person(s)?

III. What (human) oversight of the process is available?

For SYSTEM, it appears that the multivariate data analysis algorithms will autonomously trigger an alarm (i). For SYSTEM, as in many other recent security systems, it appears that algorithmic logic cannot be excluded or is involved in autonomously triggering an alarm. The combination of data or circumstances that trigger the alarm is written into the algorithm during the development of the project. They can be monitored and updated as necessary during eventual deployment. When assessing the algorithm, LEAs and public authorities should ask if the AI is to be used as a final decision maker or as an adviser to recommend certain decisions and what is the feedback process to make changes to the artificial intelligence if errors are discovered.

As far as SYSTEM is concerned, it is used, as mentioned earlier, as part of a wider investigative process. Alarms raised within SYSTEM may well initiate a procedure but with no direct significant consequences for individual persons. Areas of the city, after an alarm is raised, may be subject to further (possibly closer) surveillance by LEAs, or a police operation. But it is hard to imagine that an AI-made decision will automatically lead to a police operation: although an alarm is automatically triggered by an algorithm, further steps in the investigative process are not automated and, by contrast, involve significant intervention from investigating LEA officers. It is a fortiori hardly imaginable that any automatically raided alarm will lead to any serious legal consequences arrest, detainment, prosecution, etc.

It should, however, be considered that consequences of surveillance may not be legal ones (e.g., being arrested or otherwise caught up in a criminal investigation). There may be also consequences to do with the stigmatisation that may result from being a subject of LEA surveillance.

4. GUIDELINES ON HOW TO NAVIGATE DEVIATIONS

The category of *Deviations* covers ethical issues arising from circumstances in which there is a deviation from the 'normal' use of surveillance technology. To assess what constitutes 'deviant use' requires a relatively clear idea of what is 'normal use'.

Subcategories of the *deviations* category are:

- Function creep
- Misuse and manipulation (of technology)
- Incidental findings

4.1. FUNCTION CREEP

Function creep occurs when a technology (or technique, programme, dataset, etc.) is used for a different purpose to the one for which it was originally designed. Examples include the use by government agencies of UK identity cards, which had originally been introduced for security and rationing purposes in World War II, for reasons including collecting parcels from the post office and routine police enquiries; and, again in the UK, the use of Oyster Card (cards introduced for use on public transport in London) data for police enquiries. It must be cautioned, as also these examples suggest, that not all 'creeps' are necessarily bad; there are, instead, many advantages. In the case of SYSTEM, the potential to change sensors increase flexibility and adaptability: if different precursors or target compounds are identified as being of interest, or if new investigatory methods are developed (e.g., which rely on detection of different target substances), more suitable sensors could be substituted in accordingly. New insights on an unexpected domain can pop up, for instance, the monitoring of sewage for public health reasons related to epidemics then pandemics such as COVID-19. There is a lot of positive potentials here. That should be maximised. However, it must always be remembered that even when the 'creeps' are apparently positive, there is still a need for review, analysis, and oversight: not only positive unexpected insights but also negative unexpected problems may emerge.

4.2. MISUSE AND MANIPULATION OF TECHNOLOGY

Misuse typically refers to the use of materials, methods, technologies, or research outcomes for unethical purposes. Risks can be identified by considering what might happen if unauthorised

actors gain access to the technology or to key details about how it works or how it is intended to be deployed. Mitigations may involve steps to ensure that unauthorised access to technologies is limited, but may also involve adjusting deployment strategies to limit the impact of knowledge about the technology or its intended deployment falling into the wrong hands. What might happen if unauthorised actors gained access to SYSTEM-like technology or to key details about how it works or how it is intended to be deployed? In the most salient case, criminals running clandestine drugs laboratories could gain information about how SYSTEM works and, as a result, change their methods. This means that one effect could be to deter the establishment of clandestine drugs laboratories in urban areas, pushing production into more rural areas which might be presumed less subject to SYSTEM surveillance. This would have social and very possibly an environmental impact: on one hand, negative consequences for people living in areas the criminals relocate to, and dumping in the ground (forests, streams) toxic chemicals, on the other. Alternatively, laboratories remain in urban areas, but criminals travel to other areas, or even cross into another country, to dispose of their waste without flushing it down. There are severe environmental costs to this outcome.

4.3. INCIDENTAL FINDINGS

Questions about *incidental findings* are common in healthcare ethics, where the use of diagnostic tools and techniques is apt to uncover unexpected data concerning the health of the patient, their relatives or others. In the context of surveillance, "identity management, privacy and data protection, and the possibility of social and political discrimination raise more issues that parallel but do not equate to the possible harms in biological, genetic, and medical sciences." Policies should, as far as possible, identify likely categories of incidental findings (what kinds of data are most likely to be inadvertently collected). Arguably policies are not the ideal tool for dealing with incidental findings; prevention, i.e., measures that minimise the likelihood of incidental findings arising should be pursued (as mandated by data minimisation requirements, see data protection section).

5. GUIDELINES ON PRIVACY AND DATA PROTECTION /FUNDAMENTAL RIGHTS

SYSTEM like technologies do not intrude in the sacred domain of the house, it does not seek or process personal data, and do not create discrimination between individuals or groups. However,

risks to privacy, personal data protection and other fundamental rights may emerge should additional sensors or functionality be added to SYSTEM.

5.1. PRIVACY AND HOME LIFE

Privacy definitions convey the idea that privacy may be interpreted in a narrow sense, notably informational privacy, or the right to be left alone, or as control over one's domestic space, and in a broader sense, where privacy emerges as relating to notions of "personal autonomy", "personhood" and "decisional privacy". This broader understanding is apt to describe the potential of surveillance measures to have chilling effects on individuals. [16] The awareness of being watched, or monitored, erodes the space of individual freedom and autonomy that privacy protects. [17] Individuals may alter their behaviour, even when such behaviour is legal. Others may feel disturbed at the prospect that the police could be alerted. Some people may not only behave differently in monitored areas, but they may also as well avoid going to those areas at all. In its broader sense, instead, privacy emerges as a fundamental value of democratic, pluralistic states.[18]. Famously, Orwell's hallucinating novel 1984 portrays an unfree society where cameras installed everywhere, including in public spaces, leave no room for a single bit of privacy. In that society, where free thinking is suffocated in the cradle, there is no possibility for democratic government. In recent years, various scandals, such as those revealed by the PRISM case and the Snowden revelations, have raised the concern that surveillance technologies may proliferate out of control, i.e., with no limitation to what data security or law enforcement agencies can collect and process.

Considered as a whole, SYSTEM has no significant implications for privacy in the narrow sense, as the privacy of the domestic space. SYSTEM enables wide-area monitoring, something which is not sufficient to identify or single out particular people or apartments/houses. Concerns regarding privacy and home life may arise once particular buildings are within range of the sensors, a scenario that the project's tests and demonstrations have not contemplated. Whilst privacy is not, therefore, a significant issue in SYSTEM, Koops and colleagues raise the doubt that such monitoring could be

[16] P. Quinn and P. De Hert, Self respect—A "Rawlsian Primary Good" unprotected by the European Convention on Human Rights and its lack of a coherent approach to stigmatization?', *The International Law of Discrimination and the Law*, 14,((2014) pp. 19-53 Under the ECHR's privacy approach for example it is recognized that there is a need to protect individuals from harmful forms of hate speech.

[17] S. Gutwirth, (2002) Gutwirth for example refers to a need to reduce steering forces upon individuals which unduly pressure them to make decisions in certain ways.

[18] C. Bennet, (2011). H. Nissenbaum, Protecting Privacy in the Information Age: The problem of Privacy in Public', *Law and Philosophy*, 17,((1998) pp. 559-596

interpreted as a form of looking inside the home without entering: "[…] More importantly, sewage monitoring systems are an example of a tool that can measure 'things' (matter translated into data) that emanate from the home, and add to the situation that LEAs increasingly have possibilities to "look inside" the home without entering."[19]

This raises the challenge that the multitude of tools that can monitor the home from the outside, maybe erode rights such as privacy of the home. in this connection, according to Koops and colleagues, sewage monitoring might be considered a measure that intrudes upon home life in a *minor way*. Considering monitoring of a building by MilliMole, MicroMole, and LC/MS devices minor, does not preclude the possibility, should additional sensors or data from other sources be added, to intrude upon home life in a *major way*.[20]

5.2. PERSONAL DATA PROTECTION

In the project, the data that has been collected from sewage monitoring technologies and from other sources, namely, sensors, is not personal data; data protection would thus appear to be a very minor concern. As mentioned above with privacy, the main concern is for the potential consequences of the combination of data from sewage monitoring technologies with other data. For this reason, it is advisable carrying out a Data Protection Impact Assessment (Article 35 GDPR), prior to any deployment of a system like technology. This is a practical way to verify whether any processing of personal data takes place and to adopt adequate, legal, measures.

5.3. OTHER FUNDAMENTAL RIGHTS

The chilling effect described earlier may impact the rights to liberty. Aside from this chilling effect, however, the right to non-discrimination is unlikely to be directly impacted by the sewage monitoring technology planned in SYSTEM. Discrimination could occur in the selection of locales to be subject to wide-area monitoring, demanding that the rationales behind decisions to select areas for monitoring to be robust and clear.

[19] Škorvánek, I., Koops, B.-J., & Timan, T. (2019). Surveillance, Criminal Procedure, and Regulatory Connection: The Case of Sewage Monitoring (SSRN Scholarly Paper No. ID 3377466) p. 32.

[20] . (Koops et al., 2019, p. 11)

As mentioned above, additionally, the potential indirect environmental impact should be considered. For instance, if SYSTEM is successful, it could lead to criminals finding alternatives to disposing of the waste products of their clandestine drug laboratories in household waste: they may resort to measures with negative environmental impact, such as dumping it in secluded areas like forests (as reportedly happens in the Netherlands, for instance).

6. GUIDELINES ON SOCIAL ISSUES

The deployment of any type of surveillance system may have unintended consequences for the psychological and emotional wellbeing of those who are monitored. Different factors can contribute or be associated with the psychological and emotional conditions of surveillance, for example, what the purpose of the surveillance is perceived to be and whether the threat it addresses is perceived as real and serious, its context (e.g., law enforcement, workplace monitoring, etc.), where the surveillance takes place, whether an area is perceived to be a private or public space, whether the surveillance is overt or covert, etc. The psychological, emotional, behavioural and social issues that can arise from the introduction of a surveillance programme such as SYSTEM include:

- Stigma and marginalisation
- Psychological impact
- Social cohesion
- Reassessment of practices associated with waste discharge

6.1. STIGMATISATION

In his classic 1963 work Stigma: Notes on the Management of Spoiled Identity, Erving Goffman distinguished three forms of stigma: the stigma of the body, the character, and the tribe. The stigma associated with surveillance may fall into any of these categories, depending on the context: on who is monitored, why, and in what way. Consequences of stigmatisation may include individual harms (for example, to self-esteem), but also societal-level harms such as, for example, (further) entrenching divisions between communities and undermining trust in institutions and LEAs in particular (discussed above). Thus, in assessing the potential for a surveillance technology to stigmatise, it is necessary to consider whether the surveillance is targeted at people with specific characteristics (physical, mental, behavioural, political, religious, stemming from ethnicity, class, and so on) or if it is intended to reveal specific characteristics (of these kinds). People having those characteristics may come to be viewed with suspicion (negatively impacting their psychological wellbeing, undermining whatever pride they feel about their area – which can contribute to the decline of an area in many other respects, e.g., in terms of economics, social cohesion, and so on). All of this undermines individual psychological wellbeing and social cohesion locally, city- and region-wide.

6.2. PSYCHOLOGICAL IMPACT

Being under observation is associated with greater self-awareness, self-censoring, and inhibition (the chilling effect mentioned above regarding privacy impacts). Workplace monitoring, for example, though in some cases correlated with improved productivity, is also associated with increased levels of stress while surveillance for policing is implicated as a risk factor for psychological distress and mental health.[21] The introduction of surveillance technology may contribute to stress and affect the psychological and emotional wellbeing of people. To mitigate this risk, the expectation, and perspectives of people subject to surveillance, of those conducting the surveillance, or of people otherwise caught up in it (in the case of SYSTEM, employees of garbage collection operators) should be taken into consideration.[22]

6.3. SOCIAL COHESION

Surveillance impacts social cohesion via its impact on trust. Surveillance may be, at one and the same time, both encouraging and undermining trust. It is to some extent encouraging trust because of its disciplinary effect, promoting conformity and predictability with established norms of behaviour; and yet it undermines trust – its very presence implying suspicion and mistrust. Surveillance, especially in law-enforcement contexts, implies a degree of mistrust of at least those persons under surveillance, then, overall, such surveillance can only be inimical to social cohesion. Measures are therefore required in order to manage the impact of surveillance on social cohesion by ensuring that, as far as possible, only those people for whom it is reasonable, legitimate, and just cause are caught up in surveillance programmes; and that people who may be caught up in surveillance programmes are informed and, as far as possible, given a voice in discussions as to how best implement such programmes.

6.4. REASSESSMENT OF PRACTICES ASSOCIATED WITH WASTE DISCHARGE

The SYSTEM project does not propose to examine the contents of anyone's toilet bowl or to search through the contents of anyone's rubbish bins. But it is worth considering that the use of

[21] Sewell, A. A., Jefferson, K. A., & Lee, H. (2016). Living under surveillance: Gender, psychological distress, and stop-question-and-frisk policing in New York City. Social Science & Medicine (1982), 159, 1–13. https://doi.org/10.1016/j.socscimed.2016.04.024

[22] Consider a somewhat related case. Can social media use affect psychological wellbeing? Absolutely it can (Hampton, Rainie, Lu, Inyoung, & Purcell, 2015). But it would be mistake to focus only on the mental health of social media *users*: other stakeholders – notably content moderators – suffer a significant negative impact (see, e.g., in the case of Facebook, Garcia, 2018; Newton, 2019; Solon, 2017).

technologies such as those proposed in SYSTEM might – perhaps in conjunction with other developments[23] – serve to disrupt commonplace conceptions of household waste (of all kinds). It isn't obvious how technologies like sewage monitoring might affect the ways in which we think about sewage and related substances and activities. The kinds of monitoring contemplated in SYSTEM may seem relatively unintrusive and, given their law-enforcement aims, limited to cases in which justified suspicion is present. But it is worth considering again the sensitivity we feel about bodily excreta and household waste, as well as the doubly private nature of bathrooms and the activities that take place in them.

7. CONCLUSIONS

The guidelines are, in fact, recommendations directed at policymakers who are encouraged to take into consideration some legal, ethical, and social conditions or consequences of the deployment of SYSTEM-like technologies.

The first guideline/ recommendation is "to anticipate that transparency is needed sooner rather than later, and therefore to proactively develop a policy on what can be publicly disclosed on the operation of the system and which operational details must really be kept secret." Transparency requires oversight and control, so that the legitimacy of wide-area monitoring is ensured, and also information to be provided to the public. With regards to the latter, oversight in concrete means communication between LEA stakeholders and municipalities and specifically, elected policymaker representatives. If certain information must remain secret, this secrecy can be explained in terms of genuine security requirements and be agreed upon. In this way, legitimate security requirements and needs for secrecy are respected, while oversight and accountability, is ensured. In the latter regard, information, LEAs and public authorities are encouraged to work closely to decide whether information should be provided, how much and through which channels. Another recommendation/guideline invites policymakers to debate, in the appropriate institutional places, the necessity, the proportionality, the accuracy and the explainability of SYSTEM-like surveillance

[23] Researchers recently developed a 'smart toilet' (note that there are currently no plans to develop it commercially:

> The 'smart' toilet was developed by engineers at IMEC Nederland to show what can be measured using a WC and how that can be linked to the health of the user. […] The smart toilet includes sensors to measure heart rate and blood pressure, while urine will be analysed for temperature and salt content. 'If the salt content is too high, we can recommend they drink more liquids – or less alcohol. ('Smart toilet will suggest what you should be eating at Lowlands', 2019).

systems. The third set of guidelines invites policymakers to consider the risk of surveillance technology deviating from its original purpose or providing unforeseen insights. SYSTEM does not infringe on the privacy of homes, nor does it collect any personal data. However, the deployment of these technologies should, in any case, consider the chilling effect of surveillance on private life and assess, for instance by means of a DPIA, whether personal data is or not actually collected and processed. Finally, albeit it is unlikely that SYSTEM will generate any, surveillance does have the potential to have social and psychological impacts. Different factors can contribute or be associated with the psychological and emotional conditions of surveillance, for example, what the purpose of the surveillance is perceived to be and whether the threat it addresses is perceived as real and serious, its context (e.g., law enforcement, workplace monitoring, etc.), where the surveillance takes place, whether an area is perceived to be a private or public space, whether the surveillance is overt or covert, etc.

BIBLIOGRAPHY

- Conley, C., Cagle, M., Bibring, P., Farris, J., Lye, L., Ebadolahi, M., & Ozer, N. (2016). Making Smart Decisions about Surveillance: A Guide for Community Transparency, Accountability & Oversight. Retrieved from American Civil Liberties Union of California website: www.aclunc.org/smartaboutsurveillance
- Škorvánek, I., Koops, B.-J., & Timan, T. (2019)., Surveillance, Criminal Procedure, and Regulatory Connection: The Case of Sewage Monitoring (SSRN Scholarly Paper No. ID 3377466)
- Knowledge@Wharton. (2019, September 24). What's Fueling the Smart City Backlash? Retrieved from https://knowledge.wharton.upenn.edu/article/whats-behind-backlash-smart-cities/
- Fussell, S. (2019, August 30). Why Hong Kongers Are Toppling Lampposts. Retrieved from The Atlantic website: https://www.theatlantic.com/technology/archive/2019/08/why-hong-kong-protesters-are-cutting-down-lampposts/597145/
- Conley, C. (2017). Making Smart Decisions about Smart Cities. Retrieved from American Civil Liberties Union of Northern California website: https://www.aclunc.org/publications/making-smart-decisions-about-smart-cities
- Conley, C., Cagle, M., Bibring, P., Farris, J., Lye, L., Ebadolahi, M., & Ozer, N. (2016). Making Smart Decisions about Surveillance: A Guide for Community Transparency, Accountability & Oversight. Retrieved from American Civil Liberties Union of California website: www.aclunc.org/smartaboutsurveillance
- Froomkin, A. Michael. "Privacy Impact Notices to address the privacy pollution of mass surveillance." In Timan, Tjerk, Bryce Clayton Newell, and Bert-Jaap Koops, eds. Privacy in public space: Conceptual and regulatory challenges. Edward Elgar Publishing, 2017
- ECtHR, Uzun v. Germany, application no. 35623/05, judgment of 2 September 2010 ("Uzun v. Germany")
- Cameron, National Security and The European Convention on Human Rights, The Hague/London/Boston, Kluwer Law International, 2000
- P. Quinn and P. De Hert, Self respect—A "Rawlsian Primary Good" unprotected by the European Convention on Human Rights and its lack of a coherent approach to stigmatization?', The International Law of Discrimination and the Law, 14,((2014)

- M. Delmas-Marty, The European Convention for the Protection of Human Rights, Dordrecht, 1992
- Sewell, A. A., Jefferson, K. A., & Lee, H. (2016). Living under surveillance: Gender, psychological distress, and stop-question-and-frisk policing in New York City. Social Science & Medicine (1982), 159, 1–13. https://doi.org/10.1016/j.socscimed.2016.04.024
- Škorvánek, I., Koops, B.-J., & Timan, T. (2019). Surveillance, Criminal Procedure, and Regulatory Connection: The Case of Sewage Monitoring (SSRN Scholarly Paper No. ID 3377466)

ANNEX I TABLE OF GUIDELINES

No.	Guidelines
1	Anticipate that transparency is needed sooner rather than later, and therefore to proactively develop a policy on what can be publicly disclosed on the operation of the system and which operational details must really be kept secret (balance secrecy and transparency)
2	Transparency requires oversight and control and also information to be provided to the public.
3	Prepare a draft public engagement strategy that sets out how the public will be informed about SYSTEM (what they will be told, how it will be presented, to what extent (if any) they will have a say in how SYSTEM is deployed in their area, etc.
4	In the appropriate institutional places, debate on the necessity, the proportionality, the accuracy and the explainability of SYSTEM-like surveillance systems.
5	Brace for the risk of surveillance technology deviating from its original purpose or providing unforeseen insights.
5	Consider the chilling effect of surveillance on private life and assess, for instance by means of a DPIA, whether personal data is or not actually collected and processed.
6	Consider consulting people (or their representatives) potentially negatively affected by SYSTEM surveillance (e.g., residents of socially marginalised areas, minority groups, civil society organisations, NGOs, or community groups). These stakeholders can be a source of important

	insight for the project.
7	The accuracy and reliability of all SYSTEM component technologies should be monitored, with false-positive rates made available to authorised persons conducting impact assessments (or similar). When this information is available, impact assessments may have to be re-evaluated or updated.
8	Any alarm that could trigger events of serious consequence for any person should be reviewed by a qualified individual before the consequences are set in motion.
9	The potential indirect environmental impact should be considered. For instance, if SYSTEM is successful, it could lead to criminals finding alternatives to disposing of the waste products of their clandestine drug laboratories in household waste: they may resort to measures with negative environmental impact, such as dumping it in secluded areas like forests (as happens in the Netherlands)