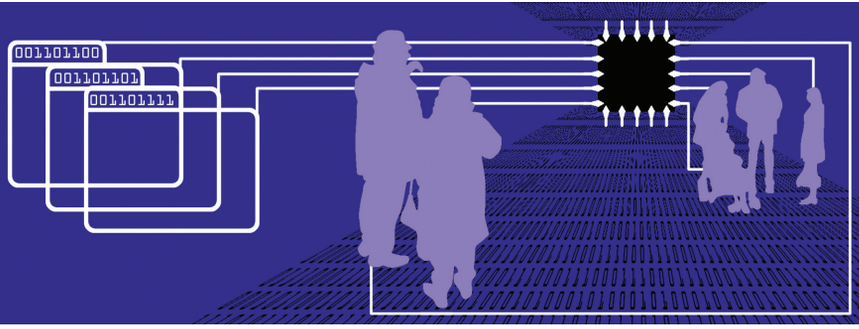


SURVEILLE

Surveillance: Ethical Issues, Legal Limitations, and Efficiency

Assessing surveillance technologies:

A nuanced approach for determining security benefits against financial costs, moral hazards and impact on fundamental rights

Key points

- It is urgent and in everyone's best interest to restore legality and legitimacy when it comes to surveillance.
- The SURVEILLE methodology can be used to determine on a case by case basis whether it is legal, moral, efficient and effective to use a particular surveillance technology.
- The SURVEILLE methodology shows that it is possible to reconcile security and privacy in a rational and structured way.

Surveillance technologies used in the prevention, investigation and prosecution of terrorism and other serious crimes are ubiquitous. However, policymakers are having a hard time weighing the actual security benefit of any surveillance technology against the potential financial cost, moral hazard, or resulting intrusion into privacy and other fundamental rights.

How can a state protect its people while eliminating moral hazards and fundamental rights intrusions? And how can policymakers cut costs without sacrificing security?

These questions are not new, but the answer provided by the SURVEILLE project might be.

This brief examines why action is needed now and proposes a new methodology that could help everyone from policy makers and police officers to judges and prosecutors to determine on a case by case basis whether it is legal, moral, efficient and effective to use a particular surveillance technology.

For the first time, this comprehensive methodology takes into account the impact of different surveillance technologies on fundamental rights like the right to privacy and freedom of

expression. At the same time, it measures effectiveness, including cost. The methodology is informed by local conditions and scenarios and will simultaneously protect people's security and fundamental rights.

It can be applied in a wide range of situations, including when:

- **drafting legislation on surveillance.**
- **deciding about the development or deployment of new surveillance technologies.**
- **deciding about the authorization of using a particular surveillance technology.**
- **in a practical situation when using the technology.**

How we got here

There is tremendous pressure on governments to deliver quick results and answers in the wake of terrible acts like the attacks at French magazine Charlie Hebdo or the September 11th attacks in the United States. While it is natural for fear and anger to set in after such incidents, and legitimate for governments to try to increase the protection of citizens, governments can overreach and enact legislation hastily, introducing surveillance technologies that affect fundamental rights protected by European and international human rights law.

The Edward Snowden revelations of 2013 have demonstrated further that modern forms of mass surveillance often lack a proper legal basis. Modern methods of electronic mass surveillance have come to represent a waste of money with very little benefit to security, while at the same time causing huge ethical problems and deep intrusions into privacy and other fundamental rights.

In short, democratic Western countries are currently engaging in poorly regulated surveillance. This is of course a legitimacy issue, as governments everywhere in the West now suffer a lack of trust. It is urgent and in everyone's best interest to restore legality and legitimacy.

The case for balance

There are many good and even necessary uses of surveillance, provided the methods are well chosen and the requirements of necessity, proportionality, legitimate aim and legal basis are taken seriously. Electronic mass surveillance has failed but other targeted forms of surveillance should be considered.

Still, governments will only be able to restore legality and legitimacy by using a more rational approach that actually improves the balance between surveillance and the protection of fundamental rights, instead of just using the metaphor of a "balance" to justify any form of surveillance.

This is not simple. Surveillance brings with it a number of major challenges. Often, surveillance affects a number of fundamental human rights. Violations of human rights can result from the use of:

- **closed-circuit television (CCTV) in public spaces or private premises.**
- **traditional interception of telephone calls or the placement of listening devices to monitor suspected criminals.**
- **electronic mass surveillance.**

The fundamental right most commonly affected with the use of surveillance technology is the right to privacy. But depending on the circumstances, many other fundamental rights can be affected by surveillance. These include freedom of movement, freedom of association, and freedom of assembly.

Beyond the potential impact of surveillance technologies on our fundamental rights, surveillance also raises a range of ethical risks. These include the consequences of error, intrusion and discrimination.

A new tool for new times

The SURVEILLE methodology has three parallel assessment procedures. These help users appraise the potential moral risks (ethics), fundamental rights intrusions (law), and efficiency (technology assessment) of a specific surveillance technology when used in a scenario. These three assessments contribute to a final overall assessment that determines whether or not a surveillance technology should be used.

Using the methodology

Is a technology efficient?

As a first step, a technology assessment is done on a particular surveillance technology, such as a phone bug or luggage scanner. This results in a usability score, which seeks to measure the contribution of a particular surveillance method to the aim of surveillance, for instance the prevention or investigation of a crime.

In the SURVEILLE methodology, the usability of surveillance technology is understood in terms of:

- **effectiveness**
- **cost**
- **privacy-by-design features (which is an approach that takes privacy into account throughout the whole engineering process of any technology)**
- **overall excellence**

The usability score ranges from 0 to 10, 0 representing the least usable, and 10 the most usable technology. The score is the sum of ten different factors, each giving up to one point.

A key concept to understand here is that a surveillance technology can only be allowed to intrude into privacy or another fundamental right if the surveillance is intended to serve an aim that is legitimate, like preventing a crime, and actually advances that aim. At this point, the usability score must be determined in relation to the benefit surveillance actually delivers.

On the right side of the law

As the next step, a **fundamental rights intrusion score** is calculated for the same surveillance technology. This is a score, on a scale from 0 to 16, which determines the impact that the use of a particular surveillance technology has upon a fundamental right. At first, it must be verified that a legal basis exists for the surveillance measure. Then two main factors are assessed on a scale from 0 to 4: the weight or importance of a fundamental right in a given context and the depth of the intrusion into that right. These assessments are based on comparing the situation with existing case law by the European Court of Human Rights or the Court of Justice of the European Union. Then, a numerical value (maximum 1) is given for the reliability of these first two assessments in light of that case law. The fundamental rights intrusion score results from the multiplication of these three factors and can range from 0 (no intrusion) to 16 (highest possible intrusion).Once the usability score and the fundamental rights intrusion score are compiled, a comparison is made between the two.

Under this approach, the higher the fundamental rights intrusion score is, the greater the usability score must be for the technology to be legitimate. The two highest possible fundamental rights intrusion scores (16 and 12) represent situations where a measure would unavoidably result in fundamental rights violations, for instance because of breaching the essence of a right. Hence, not even the highest usability score can justify the use of the particular method of surveillance in that particular situation.

In some cases – for instance electronic mass surveillance – the usability score will be so low that it will be hard to demonstrate the necessity of using that particular form of surveillance. In other cases, the fundamental rights intrusion score will be so high that no benefit towards the aim of the surveillance can make it justified. In a third, large, range of cases, the usability score is high enough to demonstrate real benefits while the fundamental rights intrusion score is not so high as to signal an unavoidable human rights violation. This is where a comparison between the usability score and the fundamental rights intrusion score will benefit from an ethics assessment.

Evaluating the ethical risks

The third step in the overall assessment is the ethical assessment of the surveillance technology. The comparison between the usability score and the fundamental rights intrusion score must be informed by the ethical risks identified in the ethics assessment.

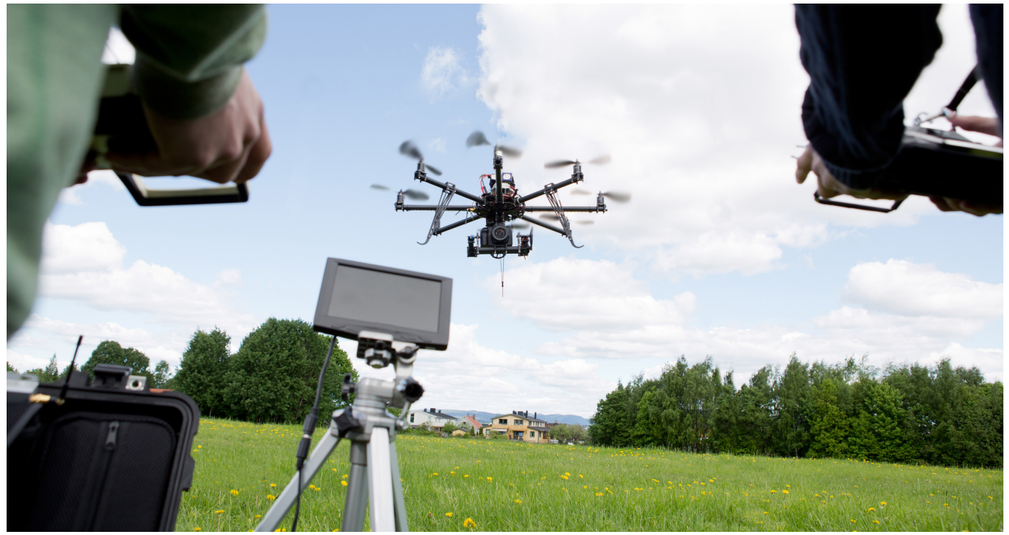
Rather than calculating a numerical outcome here, the ethical scoring uses a colour coding scheme to ethically assess the use of a surveillance technology in three separate categories.

1. **Intrusion of privacy in three distinct zones of privacy – bodily privacy, privacy of home spaces, and private life.**

2. **Risk of error such as a false positive, a user error, or data corruption that leads to intrusive searches or arrests.**

3. **Breach of ethical proportionality, meaning a surveillance technology was used which was more rights-violating than necessary for the purpose pursued.**

Moderate risks in these three categories are coded green, intermediate risks yellow and severe risks red. When the usability score and fundamental rights intrusion score are identical, or close to identical, the ethics alert may inform the decision as to whether or not to use a surveillance technology in a particular situation and context.



Examples of outcomes of SURVEILLE assessments on different surveillance technologies in three different situations

Outcome of assessment	Organised crime investigation scenario	Terrorism prevention scenario	Urban security scenario
Justified (acceptable) forms of surveillance	• Overt use of CCTV in public space • Automated detection of explosives or drugs	• Checking suitcases of cross-border traveler • Human observation (following) of suspects	• Overt use of smart CCTV in public space • Automatic number plate recognition
Questionable (suspect or highly suspect) forms of surveillance	• Covert photograpy in public space	• Social network analysis based on new social media	• Video camera mounted on drone
Rejected (impermissible) forms of surveillance	• Covert listening bug in public transport • Covert listening bug in a suspect's home	• Interception and analysis of all electronic communications passing the border (tapping of fiber-optic cable)	• Sharing of CCTV images between private businesses

A rational and structured way forward

A final overall assessment based on the results of the usability score, the fundamental rights intrusion score, and the ethical assessment is made to determine whether or not a surveillance technology should be used in a concrete situation. After answering these final questions, there are three potential results: reject, use, or go back to the drawing board.

The SURVEILLE methodology shows that it is possible to reconcile security and privacy in a rational and structured way. This is a win-win situation for society as a whole. It allows authorities to do their best to protect people – both people's security and their fundamental rights. The methodology can for instance help:

- **lawmakers ensure that**

- the requirements of legitimate aim, necessity and proportionality are actually met, instead of used as rubber stamps to justify surveillance.

- the laws will be implemented subject to clear monitoring and accountability.

- **police officers make informed choices in their procurement of technology and to make sure that a particular technology is used only in legitimate situations and in a proper way.**

- **prosecutors ensure that police actions get constant supervision and scrutiny.**

- **judges undertake real and informed review before issuing a warrant authorising a particular form of surveillance.**

- **trial judges assess whether surveillance technology was used lawfully and to disregard unlawfully obtained evidence.**

Going forward, it is possible to envisage products, such as a training course and an online tool, which enable a user, such as a police officer or judge, to answer questions from the three assessment areas so as to decide whether or not the use of the surveillance technology in the particular case at hand is effective, ethical, and legal.

This briefing note was written by Gabriel Stein (Raoul Wallenberg Institute of Human Rights and Humanitarian Law) and Martin Scheinin (European University Institute, consortium leader). For more information, visit the SURVEILLE website **www.surveille.eu**.

The findings of this research which led to the methodology emanate from a multidisciplinary collaborative research project funded by the European Commission. The partners included the European University Institute, University of Warwick, the Raoul Wallenberg Institute of Human Rights and Humanitarian Law, Delft University of Technology, Albert-Ludwig-University Freiburg, Fraunhofer Gesellschaft zur Förderung der angewandten Forschung e.V., Université Libre de Bruxelles – Institute d'Etudes Européennes, the European Forum for Urban Security, Merseyside Police, and the University of Birmingham.

SURVEILLE

SURVEILLANCE TECHNOLOGY AND CONTEXT

TECHNOLOGY ASSESSMENT USABILITY SCORE 1-10

Effectiveness (max 3)
- Delivery
- Context
- Sensitivity

Privacy by design (max 3)
- Data collection
- Data access
- Data protection

Cost (max 3)
- Initial cost
- Personnel
- Other costs

Proven technology (max 1)

10 / 5 / 0

ETHICS ASSESSMENT

Intrusion of privacy

Risk of error

Breach of ethical proportionality

FUNDAMENTAL RIGHTS INTRUSION SCORE 1-16

Verify legal basis (yes/no)

Importance of fundamental right (max 4)

Depth of right's intrusion (max 4)

Does European case law back up these first two assessments? (max 1)

16 / 12 / 8 / 4 / 0

Privacy by design

Decision Support System

Holistic overall assessment combining the three assessments including proportionality

REJECT

REVISE AND REASSESS

USE

SURVEILLE

Surveillance: Ethical Issues, Legal Limitations and Efficiency

This briefing note builds upon research conducted by the SURVEILLE project, reported, inter alia, in the following earlier publications:

- D2.1 Survey of surveillance technologies, including their specific identification for further work in SURVEILLE WPs 3-5
- D2.2 Paper with input from law enforcement end users
- D2.3 Paper by local authorities end users
- D2.4 Paper establishing the classification of technologies on the basis of their intrusiveness into fundamental rights
- D2.6 Matrix of surveillance technologies
- D2.7 Update of D2.1 on the basis of input of other partners
- SURVEILLE Paper on a terrorism prevention scenario based on D2.8
- SURVEILLE NSA paper based on D2.8
- D2.9 Consolidated survey of surveillance technologies
- D3.8 Report combining results of all effectiveness research
- D3.9 Final Report of WP3 on perceptions and effectiveness of surveillance
- D4.10 Synthesis report from WP4 on the law and ethics of surveillance technologies

Each report indicates the project partners and individuals who have contributed towards it. The research and any conclusions drawn from it shall be attributed to the individual authors of each paper.

Work is underway towards academic journal articles and other publications. Updated information and all above-listed reports can be found at **www.surveille.eu**

Funded by the European Union

This Collaborative Project received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no. 284725, for the period 1 February 2012 to 30 June 2015