IRISS
INCREASING RESILIENCE
IN SURVEILLANCE SOCIETIES

Funded by
the European Union

HANDBOOK ON INCREASING RESILIENCE IN SURVEILLANCE SOCIETIES

2014

HANDBOOK ON INCREASING RESILIENCE IN A SURVEILLANCE SOCIETY

Key considerations for policy-makers, regulators, consultancies, service providers, the media, civil society organisations and the public

Trilateral Research & Consulting LLP, with contributions from the University of Edinburgh, Eötvös Károly Policy Institute (EKINT, Hungary), Peace Research Institute Oslo (PRIO), Open University (UK), the University of Hamburg and the Institute for the Sociology of Law and Criminology (IRKS, Austria).

Suggested reference: IRISS Consortium, *Handbook on Increasing Resilience in a Surveillance Society: Key considerations for policy-makers, regulators, consultancies, service providers, the media, civil society organisations and the public*, IRISS project, EC Grant Agreement No. 290492, September 2014.

This publication is available online at:
http://irissproject.eu/?page_id=9

Project website: www.irissproject.eu

Design: Trilateral Research & Consulting LLP

Acknowledgement: This Handbook is issued as part of the IRISS project, which received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under Grant Agreement No. 290492.

CONTENTS

INTRODUCTION TO THE HANDBOOK

The aim of this handbook is to help increase resilience in surveillance societies. It is aimed at six main groups of stakeholders: policy-makers and regulators, consultancies, service providers, the media, civil society organisations and the public.

The term "surveillance society" came into widespread use, at least in Europe, with the publication of a report produced for the UK Information Commissioner in 2006. Based on that report, then Commissioner Richard Thomas warned in August 2006 that the UK was "sleepwalking into a surveillance society", by which he meant not only that surveillance was becoming ubiquitous in the UK, but that most people were unaware of its ubiquity, that there was little public debate about its ubiquity and its effects and how negative effects could be countered.

The report, prepared by the Surveillance Studies Network (SSN), defined surveillance as follows: "Where we find purposeful, routine, systematic and focused attention paid to personal details, for the sake of control, entitlement, management, influence or protection, we are looking at surveillance." It added that "The collection and processing of information about persons can be used for purposes of influencing their behaviour or providing services." But surveillance is more than that. Intelligence agencies and probably some companies not only use surveillance to discover what their enemies and customers are doing, but also to uncover the activities of their competitors, and even their "friends" and allies.

The IRISS consortium has defined a surveillance society as one in which the use of surveillance technologies has become virtually ubiquitous and in which such use has become widely

(but not uniformly) accepted by the public as endemic and justified by its proponents as necessary for economic, security or other reasons. Even if there are democratic procedures, a surveillance society is one in which there is a parallel system of power exercised by large, oligarchic companies and intelligence agencies over which effective oversight and control are largely illusory.

With regard to resilience, there are many definitions, but in the context of resilience in a surveillance society, IRISS defines it as "the ability of people (individuals and groups) and organisations to adapt to and/or resist surveillance, recognising that, while some forms of surveillance may be acceptable or tolerable, others pose a serious challenge to our fundamental rights".

This handbook is divided into three main parts. Part One provides some background on resilience in surveillance societies. It defines the terms and identifies features of resilience and today's surveillance society.

Part Two lays out a set of questions addressed to each of the stakeholder groups. The questions are intended to provoke consideration of a proposed or existing surveillance system, technology, practice or other initiative, whether the surveillance system is truly necessary or proportionate, and whether stakeholders are being consulted.

Part Three offers a list of measures that can be taken to increase resilience in a surveillance society and to restrict the scope of surveillance systems to what can be legitimately justified and to minimise the impacts of surveillance systems on the individual, groups and society.

While the stakeholders listed here are not the only ones concerned with resilience and surveillance, they have key roles in the fabric of socio-economic and political features of democratic societies. As such, these stakeholders can be considered as multipliers: by targeting them, this Handbook might benefit – indirectly – a wider group of stakeholders.

The handbook is not intended to be or replace a full-fledged surveillance impact assessment (SIA) or privacy impact assessment (PIA). However, the handbook may stimulate awareness that an SIA and/or PIA should be undertaken, especially in the context of a mass surveillance system.

PART ONE: CONTEXT

Contextualising surveillance and surveillance societies

This section outlines briefly the nature of surveillance, provides some key examples of surveillance technologies, interdependencies, surveillance players and their relationships, and illustrates the nature of surveillance societies.

A surveillance society is one in which surveillance has become virtually ubiquitous. Even if there are democratic procedures, effective oversight and control are extremely difficult in a surveillance society in which power is exercised by large companies, state organisations and intelligence agencies.

Surveillance, democracy and resilience

Surveillance can potentially offer many benefits to the state, private companies, local communities and even individuals. A democratic state can employ surveillance societies in order to help guard its citizens from terrorism, subversion and crime, to monitor its borders and to protect its national interests. Private companies can use data gathered in order to understand customers and users better, to develop better products and services and to tailor services to individuals. Communities can use surveillance to help make their localities safer or to identify those causing problems for others. Individuals can use surveillance to guard their properties or their loved ones.

Yet, whatever it's acknowledged benefits, surveillance may itself pose a threat to individuals, communities and societies, because of its ubiquity, intensity and use of personally identifiable information. These qualities of surveillance may erode privacy and a host of freedoms, rights and values that it is designed to protect, including democracy itself.

Surveillance has deleterious effects. It may affect privacy. If it is not transparent and accountable, it may erode trust, societal cohesion and even democracy itself. Surveillance's ability to discriminate amongst members of the public or social groups may have implications for social integration and societal solidarity. Surveillance also affects human dignity and challenges human autonomy. It affects the way individuals move within societies, associate with others, think, express themselves and engage lawfully in political activity. Democratic practices and the working of democratic institutions depend upon the realisation of principles, freedoms and the rule of law that surveillance is likely to threaten.

Insofar as a society is democratic, its citizens have some choice as to how their government behaves and what is permitted of companies, organisations and others. Citizens may use the electoral process or engage in public debate in order to influence governments and policy- makers. Because of the significant potential dangers involved in surveillance, surveillance policy and practice require particular public scrutiny. But as well as responding in an ad hoc fashion to problems with surveillance as they arise, societies may wish to put in place regulatory and other mechanisms in order to provide continuous safeguards against surveillance. Indeed, to some extent, this already happens. Yet one may ask how effective such existing safeguards actually are, and question the degree to which societies are currently "resilient" to the negative effects of surveillance.

Resilience to surveillance requires ways of preventing, mitigating, remedying and "bouncing forward" from the negative effects of surveillance. Resilience strategies include ways of anticipating the use of surveillance and raising the

awareness of the public. They require political actors, policy-makers and regulators to devise actions – including bringing pressure to bear, and passing and implementing legislation and other measures of control – and strategies to minimise surveillance, to make it transparent and to ensure its accountability. Resilience requires independent regulators to provide oversight, to bring sanctions to bear upon excessive surveillance and to influence surveillance plans and practices before they are implemented. It also recognises that resilience to, and regulation of, surveillance in any single country have less of a chance of succeeding without international and global co-operation and co-ordination.

PART TWO: QUESTIONS FOR INCREASING RESILIENCE IN SURVEILLANCE SOCIETIES

This part of the handbook presents questions that can be considered by stakeholders in different surveillance practices. By "surveillance practices", we refer to the information systems, devices and processes that are used to monitor people and enable their data to be gathered, analysed and applied to individuals or groups of individuals. Stakeholders in surveillance practices comprise those who conduct surveillance: service providers, governments and the consultancies that advise them. Those who seek to regulate or critique those practices, such as policy-makers and civil society organisations, are also stakeholders. The public – often the subjects of surveillance, but also those to whom surveilling authorities are answerable – are considered stakeholders as well.

The questions that follow are designed to alert stakeholders to the potential harms that may arise from surveillance practices so that they can then anticipate, avoid and recover from those harms. In other words, they can influence society's resilience to surveillance. Such harmful consequences include – but are not limited to – infringement of fundamental rights, economic and environmental harms, and social harms such as discrimination and the erosion of trust. Some questions are generic and applicable across all categories of stakeholders, while others are more specific to particular stakeholder groups. Some questions are focused upon particular systems, whereas others have a more general frame of reference concerning society at large. All stakeholders, and not only those referenced in this handbook, should ask questions about the lawfulness, necessity, proportionality and purpose of surveillance systems. They should also question their impact on

society and democratic traditions, and about the measures that can be taken to improve resilience. It is not enough simply to focus on the infringements of surveillance on individual privacy, because the effects of surveillance are felt throughout society.

GENERIC QUESTIONS

Any stakeholder can ask the following questions of any information processing system that involves personal data, whether it be an RFID-embedded travel card, a body scanner, an identification system, a data profiling system, an automated number plate recognition (ANPR) system, a location-based service, a CCTV network or a credit scoring system. A surveillance system consists of many components, technological, human and institutional. Asking questions about a surveillance system is most useful before a decision has been taken to proceed with it, as happens in a privacy impact assessment (PIA). However, many questions are also useful when scrutinising an existing system. Reflecting on such questions will help to inform stakeholders about a surveillance system, its individual and social impacts, and its social, political and legal acceptability.

With regard to the existing or planned information processing system, programme, practice or technology:

1. What is the purpose of the system?
2. Is it really necessary? Is it lawful? Is it proportionate to the envisaged purpose?
3. What less intrusive alternatives are available?
4. Who will develop, operate and authorise it?
5. Who will have access to the data collected by it?

6. How long will the collected data be stored? When will the data be deleted? What measures will be put in place to store or transmit the data securely?
7. To what extent will stakeholders, including the public, be consulted about it and its effects?
8. What external oversight is in place, including a regular, independent, third-party, publicly available audit?
9. How will system operators be trained so that they are sensitive to any harmful consequences?
10. Does the system enable individuals to be identified? If so, is that necessary? Does it provide individuals with a means to opt out?
11. Does the system process "sensitive" personal data? If so, is that necessary?
12. Whose interests does the system serve?
13. Does the system create identifiable harms, e.g., social, environmental, economic or human rights-related harms?
14. If surveillance cannot be avoided or its effects mitigated, how can society be empowered to build capacities to deal with its consequences?
15. Have the possible negative impacts and risks of the implementation or continuation of the particular surveillance system been considered? How do these relate to the benefits?

QUESTIONS FOR POLICY-MAKERS AND REGULATORS

Policy-makers and regulators, including political parties, legislators and the courts, play a crucial role in arbitrating the use of surveillance. They are able to develop the legal framework and other instruments for keeping surveillance within limits that express the principles and values of democratic society. The questions below are among the most important ones upon which these actors need to focus in shaping their legislative, administrative, judicial or regulatory activity. To a certain extent, these questions may already form part of policy-makers' operational and deliberative practices. They are presented with a focus on resilience. These questions are not offered as a "check-list" for policy-makers and regulators, but rather as a trigger for more reflective self-interrogation and modification of practices. They will enable policy-makers to consider the wider consequences of surveillance.

1. Is the surveillance necessary, legitimate, transparent and proportional? How are these judgements made? Are there any less intrusive alternatives?
2. How has the decision to use surveillance weighed up the costs, benefits and risks, including the consequences of surveillance for human rights, freedoms and democracy? Is the decision-making process publicly documented?
3. What deliberations have taken place concerning the necessity and proportionality of the intrusion into individuals' private lives by means of the surveillance measure or policy? Is the decision-making process publicly documented?
4. How have the views of different stakeholders, especially the public, been taken into account?
5. Have policy-makers identified potential harms – who is harmed by and who benefits from surveillance,

what are potential knock-on effects, what are the social consequences? After trying to identify all of the consequences, have policy-makers thought about what they can reasonably do to combat those harms?

6. What systems are in place for adequate supervision, review and oversight of surveillance practices?
7. Have the targets of surveillance (which may be the general public) been informed of the existence of the surveillance system and its general purpose? How can they find out more about the scope of the system? How can they seek personal redress for harm? How can they question, or fundamentally challenge the surveillance system?
8. How can the political and policy-making process best control the proliferation of surveillance?
9. If surveillance cannot be avoided, how can society be empowered to build capacities to deal with its consequences?
10. How are the effects of surveillance to be continuously assessed or monitored?
11. How can international regulatory co-operation and standardisation best meet the challenge of the global flow of personal information?
12. How can the political and policy-making process best control the proliferation of surveillance?
13. How can policy-makers and regulators co-operate to promote surveillance-minimising good practices (or responsible surveillance) at the international level?

QUESTIONS FOR CONSULTANCIES

Here, the term "consultancies" applies to a wide range of enterprises, from law firms to lobbyists, strategists, media advisers and researchers. Consultancies are an interface between industry and regulators and represent a stakeholder group that does not get much visibility. Consultancies primarily serve the interests of their clients, who may have vested interests in introducing technologies, products, services or other practices that are surveillant in nature. Furthermore, consultancies are often required to exercise professional judgement in their advice to clients who are introducing new information systems, or modifying or extending old ones that have a surveillance capability. As a matter of responsibility and risk reduction, consultancies can help increase resilience to surveillance by reflecting on its harmful consequences and by advising clients accordingly. Not only are consultancies responsible for providing ethical advice, but also they should know what to do if they are subject to scrutiny themselves: they need to consider how they manage their own information-processing practices.

1. Does the consultancy provide advice that respects and does not infringe the rights and freedoms of individuals? Does the consultancy adhere to a specific code of practice? Could the code of practice be used to consider the likely impact of new or existing surveillance practices?
2. Has the consultancy fostered engagement with other stakeholders? If so, how?
3. Has the consultancy conducted a surveillance or privacy and data protection impact assessment? Did it recommend engaging with stakeholders as

part of the PIA or SIA process, publishing the report and submitting it for independent, third-party review?

4. If the consultancy's advice to its clients were to be made public, would it withstand public scrutiny?
5. Does the consultancy draw to the attention of its clients the need to comply with legislation and to consider other privacy or ethical risks?
6. Does the consultancy contact regulators with the consent of its clients in order to have a view from the regulator with regard to any potential regulatory issues relating to the use of surveillance?
7. Does the consultancy advise its clients on how civil society organisations or the media might react to its clients' plans to develop a new surveillance system?
8. Does the consultancy consider the potential harms and consequences of its advice regarding a surveillance system?
9. Does the consultancy counsel its clients about measures that they could take to avoid or minimise the privacy and other risks that could arise from the proposed surveillance system?

QUESTIONS FOR SERVICE PROVIDERS

This handbook uses the term "service providers" to refer to private sector organisations that offer goods and services to customers. Service providers in the retail, communications, social media, travel, financial services and other consumer sectors routinely gather and analyse data about their customers, as well as about other aspects of their operations. This information is then used to inform business processes and to differentiate between consumers. This is done in order to target consumers with products and services. Because this targeting process (called "customer relationship management" or "CRM") gathers information that is then used to influence consumer buying behaviour, it is surveillant in nature. In some of these sectors, such as social media, the analysis and sale of customer data is the core business model. Some business sectors, such as travel, communication and financial services, are required by law and/or court orders to pass customer data to the government for national security purposes. This raises a set of concerns not only about data sharing and use of customers' data, but also about how customers perceive brands, products and services.

To increase resilience to surveillance, service providers can reflect on the following questions:

1. Has the service provider undertaken a privacy impact assessment (PIA) in relation to the customer and business information-processing it provides?
2. Is the profiling and/or monitoring of consumer groups (for example, of their behaviour, intention, sentiment, location or movements) intrusive? Would the service provider be comfortable if this profiling

or monitoring was applied to his or her family and friends?

3. How are consumers made aware of their data protection and privacy rights when they purchase a product or service from the service provider? Has the service provider made consumers aware of the extent to which it processes information about them? What measures has the service provider taken to enable consumers to contact the service provider for clarification about the information collection, processing and sharing it undertakes?
4. How easy is it for consumers to locate the data protection officer in the service provider's organisation and to make a request in respect of the information that the service provider holds on them? Is the service provider devoting adequate resources to ensure its compliance with data protection regulation?
5. In what respects could the service provider improve data protection compliance within its organisation (for example, in relation to data anonymisation, retention, storage, consent, security or data protection training)?
6. Is it appropriate for the service provider to undertake branding or marketing activity that reinforces privacy as a brand value? How might this benefit its market position?
7. How would consumer trust in the service provider's products or services be affected if it were revealed that the service provider had collected and shared information about consumers without their knowledge? What is the likelihood of this occurring?
8. In respect of the service provider's organisation, what mechanisms of redress are available to customers whose information is incorrect, or has

been wrongly or maliciously processed or shared? To what extent are the service provider's customers aware of those mechanisms? Are they made explicit on the organisation's website or in documentation sent to customers?

9. Can the service provider envisage how the receipt of lower quality or higher priced offers, based on customer profiling, may adversely affect the lives of different groups of consumers? What alternatives are available for disadvantaged consumer groups?
10. Would the service provider's segmentation criteria be legal when compared to the gender, race, disability and age-related discrimination legislation?
11. If the service provider is required to pass customer information to its national government, under what circumstances and with what effect can it refuse to comply with these requests? Has it ever done so?
12. Has the organisation been adequately resourced to deal with government requests for information?

QUESTIONS FOR THE MEDIA

Although "the media" can refer to specific entities or groups (including social media), in the context of this handbook, the media is equated with the mass media in a modern society, namely, newspapers and journals, television, radio and other forms of electronic communication. The term could also include all of the channels of communication within a society and between societies, as well as the channels that do not reach out to many people at once.

The media is of great cultural, economic and political importance in society, and the concept of a free press is a cornerstone of modern democracy. The media is especially influential in the creation and shaping of public opinion. This influence is also exerted upon executive, judicial and legislative powers, manifested by the democratic oversight and reporting by journalists exercising their right and duty to scrutinise. Furthermore, based on their power, the media is sometimes referred to as the "fourth branch of government". With regard to surveillance, the role of the media can be considered as two-fold: first, the media can be seen as a surveillant power, with the responsibility to question and report on the central constituent powers in the society. Second, the media may engage with the concept and practice of surveillance, by raising awareness and building knowledge of surveillance and resilience to surveillance in society.

1. What information concerning the (proposed) surveillance systems is available to the public? Is the information sufficient, and are the sources diverse enough, to carry on journalistic research? Are there institutional ways to obtain further relevant information?

2. How can I use my journalism as a tool for knowledge-building and awareness for those within the scope of the surveillance?
3. Am I contributing to the expansion of surveillance practices through my work?
4. Am I devoting enough attention to alternative or dissenting views with regard to a (proposed) surveillance system, policy or practice?
5. How can I build on international events and development regarding surveillance practices to draw attention and raise awareness in my own national context?
6. How can I contribute to a higher degree of awareness by shedding light on the widespread nature and impact of surveillance in society?
7. Are there changes happening in my national context of which it could be important for the public to be made aware, even though the topics may not be well received by some policy-makers?
8. How is surveillance understood in my society? Could there be a need for a debate about the very content of the term?
9. How can I engage with relevant authorities in my country, such as the Data Protection Authority and/or Surveillance Commissioner, with the aim of building resilience within the population?
10. How can my journalism encourage and facilitate public debate about surveillance issues?
11. What are the obstacles I face in investigating surveillance practices, and how can I best overcome them?
12. How can I most effectively play a role in voicing concerns and stimulating public debate about surveillance issues, e.g., sharing information or collaborating with civil society organisations?

QUESTIONS FOR CIVIL SOCIETY ORGANISATIONS

In the context of this handbook, we regard civil society organisations (CSOs) as those non-profit, non-governmental organisations concerned with and by surveillance practices, including CSOs that focus on privacy and human and fundamental rights as well as those that may be impacted by surveillance activities. Examples of the latter may be trade unions and student associations. CSOs include formally established organisations as well as those that have no formal institution – for example, ad hoc groups formed in response to a specific surveillance practice or issue.

Civil society organisations are an important link between individuals and other stakeholders, from political institutions to companies and the media. While their degree of institutionalisation, and their ability to mobilise resources and political and media attention vary widely, they offer a forum for discussion by participating individuals, and potentially a platform to require further information and advance claims.

1. Are we sufficiently informed about the (constantly evolving) nature of surveillance and its effects to be able to analyse surveillance policies and implementation of surveillance technologies? How can we improve our information resources?
2. Do we have the means (adequate information and knowledge) to discern whether and how new surveillance measures may touch upon society? Do we have the means to assess the potential consequences of these measures?
3. Have we developed adequate resources to promote greater public awareness of surveillance and means of resisting surveillance? How can we improve these resources?

4. Are we aware of the institutional and non-institutional means to resist and overcome surveillance? Do we have access to these means, or do we have the relevant skills?
5. Can we exercise any influence to resist the introduction of new and objectionable surveillance measures, by either the government or companies? How?
6. Have we contributed to the formulation of public policies (e.g., via consultations) such that surveillance concerns and threats are taken into account? Are we able to assess the impact of these contributions, and can we improve them?
7. Have we engaged in any activities that help oppose surveillance – e.g., boycotts, campaigns, complaints, court challenges, demonstrations? Did we make an impact on the decisions? Have we developed specific skills?
8. How is the surveillance policy perpetuating vulnerabilities of our societies, contributing to the frailty of our democratic practices?
9. What are the obstacles to our engagement with surveillance issues, and how can these best be overcome?
10. How can we most effectively play a role in voicing concerns, stimulating public debate, and exerting policy influence in relation to surveillance issues?
11. Are we helping those who have been harmed by surveillance (e.g., by providing a platform for voicing grievances and supporting their efforts to gain redress)?

QUESTIONS FOR THE PUBLIC

Surveillance can be directed at places, events, traffic, crowds and even animals. However, the most important and most sensitive target in the context of a democratic society is the individual. Information about individual consumption patterns, communications, financial transactions and location, among other things, is stored and analysed in the information systems of service providers and government departments. Surveillance becomes part of the fabric of everyday life and systems that are surveillance-capable become the means by which things get done. Most of this surveillance takes place out of sight of the individual, who is generally not aware of how the collected information is gathered and/or used. Because many surveillance practices also confer benefits and convenience, such as expedited travel, location-based services or customised offers, the public tends to overlook their harms. The public then becomes accustomed to living with surveillance. As the mechanisms for public scrutiny, such as subject access requests or freedom of information, are inaccessible to many, surveillance becomes disregarded as an issue. However, as soon as the negative consequences are felt – unwanted exposure in social media, refused credit, loss of privacy, loss of trust in government – members of the public become aware of their involvement. To increase resilience to surveillance, the public is encouraged to ask the following questions to help mitigate, avoid and combat the harmful consequences of surveillance practices.

1. What are the impacts of the proposed (or existing) surveillance systems on my life, the life of my family, my community, my society?
2. How can I find out who is responsible for the surveillance system, how it works and for what my information is used?

3. How and where can I find out more about the effects of surveillance upon privacy and freedoms as well as the ethical and social issues it raises?
4. How can I learn more about protecting my privacy and other fundamental rights while retaining all of the benefits of modern information technology?
5. How can I influence the deployment and use of a surveillance system? How can I object to any unacceptable or unlawful use of surveillance?
6. To whom can I complain if I find surveillance unreasonable, exaggerated, humiliating or discriminatory to me, my family or others?
7. How can I contact my elected representatives, or any organisation representing my rights, in matters of unacceptable surveillance plans or practices? Are there public consultations or campaigns in which I could participate?
8. What other measures can I take in response to surveillance that infringes my rights?
9. How can I best control information about me (e.g., about where I am) when I am online? How can I better protect my privacy when online?
10. Might my use of surveillance devices (e.g., mobile phone, video camera) infringe the privacy of others or their rights? If so, how should I address this?

PART THREE: MEASURES FOR ENHANCING RESILIENCE IN SURVEILLANCE SOCIETIES

POLITICAL AND REGULATORY MEASURES

In this section, we focus upon political and regulatory measures that could be put in place for enhancing resilience to surveillance. They relate to the questions for policy-makers and regulators identified in Part Two, most of which involve accountability, oversight, principles, and public awareness. In this Part, these items are seen in terms of the role they play in maintaining or increasing resilience to surveillance.

ACCOUNTABILITY AND OVERSIGHT

As mentioned above, resilience to surveillance requires ways of preventing, mitigating and remedying the negative effects of surveillance. The opacity and non-accountability of much surveillance needs to be overcome in order to enable these effects to be realised. Resilience includes strengthening laws and procedures for accountability and transparency through political processes that include review, the exertion of pressure from outside and within the institutions of politics and government, legislation or other formal rules, the creation of independent oversight and sanctions, and the replacement of a culture of secrecy and public acquiescence by one of openness and criticism. Accountability is more than the assignment and acceptance of responsibility for surveillance practices; it also requires procedures and rules for reporting publicly and engaging in possible challenge to the account given. Oversight encompasses part of this latter requirement, insofar as oversight is applied by specialised independent agencies on behalf of the public. Accountability and oversight in any single country will be less successful without international

co-operation and co-ordination where surveillance activities involve other countries.

Several of the generic questions in Part Two can be seen through the lenses of accountability and oversight. Policy-makers and regulators should consider measures that clarify and reinforce current legislation, compliance and "best practice" guidance with regard to the way in which system providers and users demonstrate their accountability in terms of answering the generic questions posed above. These questions closely resemble those that system developers need to answer when they conduct privacy or surveillance impact assessments, which legislators and regulators should encourage where they do not already exist as a statutory requirement. Answering these questions and giving accounts of performance are more likely to have traction on practice if they form part of oversight regimes exercised by regulators or their third-party agents. Policy-makers and regulators should consider how this oversight can be made more effective.

The questions as to how societies can best anticipate future challenges from surveillance, especially in relation to politics and policy formation, are more directly addressed to policy-makers when they develop policies or laws that involve extension or intensification of surveillance, for they ask about the consequences for power imbalances and for societal resilience to surveillance, and about ways of controlling surveillance, which includes oversight. These questions also should be answered by regulators, such as data protection authorities, concerning their own practices in carrying out their enforcement, guidance and awareness-raising roles, and in their practical activities at international levels.

CONSENT

The issue of consent is important both in the narrower sense of individual consent, but also in the broader sense of societal agreement that the state be allowed to undertake surveillance on the people's behalf. Individual consent is not an absolute requirement for the lawful processing of personal data, although obtaining consent is highly desirable for the establishment of confidence between individuals and surveillant data-collectors. Consent in regard to mass surveillance systems is problematic, especially in the public sector where surveillance is carried out for purposes of law enforcement and combating criminal and terrorist activities. The questions raised above, however, go some way towards addressing transparency even if consent is not possible. For the private sector, where dataveillance is used for marketing and other commercial purposes, required procedures for gaining consent already exist but are not always complied with. Policy-makers and regulators should consider how compliance could be improved, whether by increased penalties and sanctions for non-compliance or by more effective ways of promoting good practice. Where it is not possible, accountability and oversight are all the more necessary. It is important too that society's consent to surveillance be sought, since, while states may be able successfully to implement secret surveillance schemes, once revealed, they risk threatening the legitimacy of law enforcement and indeed the political process more generally.

STRENGTHENING LEGAL AND CONSTITUTIONAL PROTECTIONS OF PRIVACY

Regulators should ensure that surveillance systems respect privacy principles, for example, those referenced in the

proposed EU Data Protection Regulation and already in play in privacy laws around the world. Principles play a part in resilience by providing a normative rationale for judging the acceptability of surveillance, on the basis of which opposition or adaptation may take place. However, privacy is more than data protection: it includes the protection of bodies, spaces, movement, thoughts and other types of privacy and freedoms from the incursions of surveillance technologies, policies and practices. Thus, when assessing surveillance systems, regulators should take into account this wider canvas when assessing the legitimacy and legality of surveillance systems. Equality is an important principle in a democratic society, providing a further rationale for resilience or resistance and a criterion for evaluating surveillance. Surveillance may lead to discrimination and adverse decisions taken against individuals and groups in ways that cut across important values of fairness, equal treatment and the rule of law, beyond any invasion of privacy itself. Generic question 12 and questions 2, 4 and 11 for policy-makers and regulators highlight the relevance of principles and their relation to the proportionality, necessity and consequences of surveillance, all of which should be taken into serious consideration in policy-making and decisions about the legitimacy and exercise of surveillance.

DELIBERATION

When new surveillance measures are being considered, or when existing schemes are being expanded, the deliberative and democratic process should be as open, consultative and fair as possible. This is the case both in relation to small-scale local measures as well as to national (or even transnational) systems. The deliberative process enables the voices of different parties and interests to be heard, which is important

not least because the consequences of implementing surveillance schemes are potentially damaging and far-reaching. Through consultation processes, especially where these involve genuine deliberation and frank public discussion, the grounds on which the surveillance is to be introduced can be heard and assessed, and concerns and objections can be addressed. Deliberative processes facilitate public engagement and are likely to confer greater legitimacy on the surveillance schemes thereby developed.

AWARENESS AND COMMUNICATION

Raising public awareness contributes to resilience by disseminating important information that provides a platform for debate and change. If it is not known who is operating a surveillance systems or the extent of surveillance, it is not possible to resist or to be resilient. Raising awareness is a resilience measure. It is already practiced by regulators such as data protection authorities, and is addressed by questions 2, 3 and 7 for policy-makers and regulators, as well as by the generic questions that underpin the accountability procedures set out in privacy impact assessment, as mentioned above.

TEST OF PROPORTIONALITY

In Europe, the most acknowledged method of legal evaluation of conflicts of fundamental rights and legitimate interests, such as privacy and security, is the test of proportionality. The strict methodology of the test is routinely used by courts, including the European Court of Human Rights (ECtHR), when the courts make decisions on the justifiability of concrete cases of restricting fundamental rights, such as the application of surveillance measures. If the legitimacy of surveillance is questioned, the dispute in most cases is resolved

by courts, applying the test of proportionality. In the practice of the ECtHR, the emphasis is laid on the last phase of the test, that is, the moral balancing between competing rights and interests. In order to strengthen the legal requirements of introducing or maintaining surveillance measures, European courts need to lay more emphasis on the first phases of the test, namely, the factual elements of the test of proportionality.

The same methodology can also be adequately used at the level of planning, introducing or increasing individual surveillance measures, as research results from the EC-funded PRISMS project (http://prismsproject.eu) have shown. Regulatory or self-regulatory measures should be taken in order to encourage (in certain cases, oblige) stakeholders, who are interested in introducing surveillance methods, formally and substantially to apply the methodology of the test of proportionality. Elements of the test are highlighted above in Part Two, both in the generic questions and in the questions formulated for policy-makers.

INDIVIDUAL MEASURES

As the subjects of surveillance, individuals, their families and informal groups may develop strategies and ad hoc measures to mitigate the negative effects of surveillance at the individual level. One part of these strategies and measures can be regarded as *resistance,* another part as *resilience* towards surveillance. The two notions, resistance and resilience, are partly overlapping and sometimes difficult to distinguish; however, resistance is understood as active opposition, protest, "fighting back", while resilience as a property of the individual or group makes them capable of tolerating stresses and shocks, recovering from these harmful impacts and learning from earlier experience.

The precondition of resistant or resilient measures is that the affected individuals *perceive* surveillance, or perceive the surveillant elements in their everyday lives. Some forms of surveillance, such as the use of polygraphs or body scanners, are easy to comprehend, while widely used forms of computer communication and Internet use may not reveal their inherent surveillant elements to most users. It is important that the subjects of surveillance, even if they are unable to oversee all possible implications of surveillance practices, be aware of the *potential* of the surveillance practice concerned.

RADICAL SOLUTIONS

On the side of active protest, some people may destroy CCTV cameras, generate black-outs or use microwave jamming to distort communication channels of surveillance equipment. No matter how spectacular these militant actions may be, the perpetrators are committing criminal offences.

Those who prefer to stay within the borders of legality may still choose a radical solution: retreating from modern urban society, living in remote rural areas, hiding from satellite photography, not using the Internet and mobile phones – however, such solutions might result in disproportionate disadvantages to such individuals and other members of society.

People who, for whatever reason, do not want to be subjects of face recognition systems and thus social sorting may use hats and sunglasses to cover their faces; demonstrators sometimes use identical masks in order to make themselves unidentifiable.

Activist-minded people, or NGOs acting on their behalf, may call other people's attention to CCTV cameras or other

surveillance practices, making them visible or even ironic or laughable.

RESILIENT ATTITUDES

People who do not want to give up the advantages of modern information and communication technologies may still choose not to use tracking services or smartphones, unless it is really necessary for them. Others, who are aware of the profiling capabilities and techniques of service providers, may occasionally give false data about themselves where giving real names and other personal details is not a precondition of using a particular service.

Users of modern services need to consciously distinguish situations when they really need targeted and custom-tailored business offers and when this is not necessary or even disadvantageous to them; they need to distinguish cases when they really need location-based services, such as finding a nearby shop, and when they do not want to be tracked. In the latter case, users should switch off tracking devices and applications, log out from temporarily unnecessary networks or remove the battery from their phones. People who use passports or other ID documents with built-in radio frequency identifiers (RFID chips) should use a protective cover (known as a Faraday shield), which avoids unnecessary identification and tracking, and open it only when it is necessary to use the document.

A simple and customary way of reducing the level of profiling of mobile phone users is to use multiple phones and swap the pre-paid cards between their own phones and the phones of others. Pre-paid cards provide fewer possibilities for profiling than subscription phones.

PRIVACY ENHANCING TECHNOLOGIES

Users of Internet-based and/or mobile networks and services should be aware of, and use, privacy enhancing technologies (PETs) and services. Some PETs help users to mitigate individual harmful effects, offering, for example, cookie management tools, anonymous browsing options, non-tracking search engines or snoop-proof e-mails. Other PETs offer system-level solutions, such as the TOR network, which provides anonymous communication channels, or the so-called private or attribute-based credentials, which allow individuals to use only the necessary amount of identifying information required for using a service. The third group of PETs, visualization programs and applications – such as the ones which show the real route of e-mails or reveal what others can see about you on the Internet – do not solve any practical problem in relation to surveillance but make them visible, thereby helping the users to make informed decisions.

In general, a conscientious citizen living in an urban environment, and a conscientious user of modern communication services, should not live under the "tyranny of convenience". In order to mitigate harmful effects of surveillance, she should be able to fade into the mass of users, to be part of a large anonymity inside of which everybody has the same attributes. She should also be careful not to infringe other people's privacy or dignity simply by using convenient and trendy equipment, for instance, by taking pictures of her neighbours and posting them on social networks.

In sum, individuals must not develop paranoia when using services with surveillance capacities, but should have a realistic sense for judging the benefits and harms of surveillance, as well as their longer-term implications. With this approach, they can actively reduce the negative side effects

of surveillance technologies and equipment in their own local or virtual environment.

SOCIETAL MEASURES

The opinions and actions of opinion leaders, celebrities, teachers, activists and artists can have an impact on a societal level. As an outstanding example, Edward Snowden's brave disclosure of the secret services' mass surveillance practices conducted far beyond the constitutional and legitimate borders was a revelation for many people and generated critical opinions worldwide.

If such impacts promote the critical evaluation of surveillance and the clear distinction of its advantageous and harmful effects, then the activities of these influential persons can contribute to making our present surveillance societies more democratic, more lawful and ethically more acceptable. Conversely, if such personalities, driven by interests or conviction, exert an opposite influence on public opinion, then their views may reinforce the disadvantageous impacts and harmful effects of surveillance. That is why society's critical thinking and reactions are of utmost importance in such matters.

INDIVIDUAL RESPONSES AS COLLECTIVE ACTIONS

If many individuals respond the same way to the same surveillance challenges, they can exert a societal influence even if they are not organisationally co-ordinated. Certain free services, such as Change.org, can facilitate the collecting and forwarding of such responses of individuals. Virtual advocacy networks and blogs publicising surveillance practices may be regarded as intermediate forms between individual and

organised responses; however, organised collective actions or protest movements can also grow out of such individual responses.

A less spectacular but rather efficient kind of individual response exerting large-scale impact is the consequent change of consumer behaviour. If users of Internet-based and mobile services preferred less surveilling (or more privacy-friendly) services and service providers, or boycotted privacy intrusive ones, despite seemingly advantageous marketing offers, such actions would certainly change the business model of such services, resulting in the decrease of the harmful side effects of surveillance.

DEMONSTRATIONS

Demonstrations against surveillance belong to the most radical and spectacular forms of societal measures, which can have a direct impact, amplified by the media, on legislation and regulation, and their enforcement, as well as on public opinion and individual behaviour. Since surveillance itself, and in particular the asynchronous use of personal data in computer networks, is an abstract notion, members of the public may have difficulties in understanding its nature and implications. Civic organisations may act as intermediaries and help people understand surveillance practices and organise demonstrations, as happened in Germany where tens of thousands of protesters demonstrated on the streets of Berlin against the EU Data Retention Directive and against surveillance.

SPECIFIC GROUPS WITH A BIG IMPACT

Certain social and professional groups may have an impact on surveillance societies bigger than their proportion of the population. One such group is the community of IT professionals. As Lawrence Lessig famously noted, in modern information societies, "the Code is the law", that is, the de facto lawmakers are the coders: the IT specialists who design, implement and maintain information systems, including surveillance systems. This is why other members of society need to learn, and influence, their views on this subject matter. Studies of IT professionals' views on surveillance have shown that these professionals are more critical towards built-in surveillance capabilities of the information systems they are required to design and operate than may be generally assumed. It is therefore important to demonstrate to these specialists that society expects them to create a world through the systems they design in which they would happily live as private individuals, too.

Similarly influential can be the non-governmental organisations specialised in information rights and freedoms, or consumer protection groups, together with their supporters, not only through organising demonstrations but also through publicising the location and functioning of CCTV cameras on their websites, as has happened in Milan and Budapest, among other cities.

SURVEILLANCE AND DEMOCRACY

The two notions, surveillance and democracy, can easily be regarded as contradictory, even antagonistic. However, as Haggerty and Samatas (2010) show, there exist surveillance practices that may fit into a democratic, rule-of-law society,

provided that such systems comply with the fundamental legal, ethical and procedural requirements of such societies. In addition, the connotation of surveillance is different across countries and cultures, as are the social and political traditions even in liberal democracies. Citizens of former dictatorships or authoritarian regimes may be less sensitive to surveillance practices, or concentrate only on state surveillance while being negligent towards new business-driven forms of surveillance. However, a lower level of sensitivity in society does not decrease the responsibility of those who introduce or operate surveillance systems, with special regard to globalisation trends that decrease differences among surveillance techniques, practices and ideologies worldwide.

SOUSVEILLANCE, EQUIVEILLANCE

An activist approach rather more idealistic than a realistic societal measure is the so-called "sousveillance", that is, surveillance from below, or counter-surveillance, or "watching the watchers". While it is an inevitable component of a transparent and accountable surveillance system to provide channels through which the subjects can receive information about the surveillance practices, such actions, mainly in the domain of visual surveillance (for example, demonstrators using their mobile phone cameras to photograph police using cameras to surveil protestors), may serve as an awareness-raising tool rather than a real societal response to surveillance which, according to their proponents, would finally reach an equilibrium of surveillance powers, "equiveillance".

SURVEILLANCE AND ART

The positive and negative ideas constructed about surveillance, curiosity and fear, trust and distrust, relationships

between individuals, between state and society, are reflected in the media, popular culture and various artistic genres. Successful mainstream films, fiction and non-fiction can have a significant impact on public opinion, thus indirectly on the regulation and practice of surveillance. Although the "Big Brother culture" of reality shows may downplay the serious nature of surveillance, socially responsible art films, together with advocacy or activist films, may counterbalance this effect. There are artists, works of art and even artistic genres whose central theme is surveillance and being under surveillance. This specific branch in contemporary art is often called Surveillance Art, and its creators surveillance artists. Experimental films and alternative art have a relatively small and specialised audience; however, they can also have an impact on people's approach toward surveillance at the societal level.

PUBLIC OPINION

Surveys, quantitative and qualitative methods of measuring public opinion, constitute an important element of democratic governance. Pro- and anti-surveillance interest groups and advocates equally like to refer to the findings of such surveys. Pro-surveillance forces are particularly keen on quoting survey results proving that people do not take an interest in protecting their private sphere and do not oppose increasing surveillance practices. However, as Raab and Szekely have shown in the EC-funded PRISMS project, both the media and various interest groups have a tendency to cherry-pick the research findings that best support their own views, and to accept these partial results as scientific evidence.

In addition, in a democratic society there are limits even to majority opinions, policies and regulations must not reflect the

majority's views exclusively. Not infrequently, the minority must be protected from the majority and, under some circumstances, it may even become necessary to defend certain fundamental values, such as privacy, against the majority public opinion.

AN ACTIVIST PRESS

The free press is a precondition but is not in itself a satisfactory safeguard against the harmful effects of surveillance practices. Since the media in liberal capitalism is often subject to financial and other influence by the government and business entities, including those who have vested interests in increasing surveillance, the presence of an activist-minded press is indispensable for making these practices known, accountable and subject to criticism.

*

Societal measures are interrelated with both regulatory measures and the behaviour of individuals. All these potential measures can contribute to influencing regulation, enforcing transparency and accountability of surveillance, and tilt power asymmetries more toward individuals.