Tailoring responsible data management solutions to specific data-intensive technologies

Authors:

Gemma Galdon Clavell (PhD, public policy) & Leticia Duboc (PhD, computer science)

Eticas research & Consulting

Barcelona (Spain)

Abstract

The development of security and surveillance technologies produces externalities, both positive and negative. But how can these be measured and how can impacts on different stakeholders—such as citizens—and their perspectives be taken into account? And how can these broader understanding of individual and collective impacts be translated into anonymization techniques and responsible data management practices?

There are various methodologies and disciplines that have attempted to tackle the challenge of taking into account legal, social and ethical concerns in technological development, such as Privacy Impact Assessments, Constructive Technology Assessments or Responsible Research and Innovation principles. However, a method that addresses the specific needs of data-intensive security technologies and/or that goes beyond recommendations to translate societal concerns into technical specifications in a systematic manner has not yet emerged. The objective of this contribution is precisely to show how anonymization can only be built as a technical solution when societal concerns (desirability, acceptability and ethics) have been explored and taken into account.

Drawing on tools developed elsewhere, and combining them with these specific challenges, this paper proposes a four-part societal impact assessment (SIA) methodology for the assessment of security and surveillance technologies that is sensitive as much to the technological and economic concerns of engineers and decision-makers as to the societal values and the perspectives of citizens. In the method proposed, data management (and the anonymization techniques that are required for a specific project) is both the problem and the solution. To make the case, the paper draws on ongoing research from several FP7 projects where Eticas leads an 'Ethical Work Package' as well as experience in the assessment of the anonymization needs of several real-life technologies and projects.

Societal impact assessment is the evaluation of the risks, externalities and consequences of technologies, policies, programs, and systems. As a result, it must account for a wide range of concerns and stakeholders. The paper's first main contribution is to suggest a four-part approach to SIA that can help to assess data-intensive technology used for security. This framework includes many of the terms and concerns included in previous methodologies, but give them coherence, adapt them to the challenges of new technological developments (such as Big Data) and puts forward a specific assessment method to guide decision-making. The framework is based on four

main pillars that combine technological policy and sociological perspectives and inputs: desirability, acceptability, ethics, and data management, and provides a means of operationalizing assessment of security technologies to anticipate and compare a range of economic, data and values impacts for various stakeholders (see Figure 1).

D
DESIRABILITY
A
ACCEPTABILITY
E
ETHICS
Dm
DATA MANAGEMENT

Figure 1. The four pillars of a Societal Impact Assessment

1. The **desirability** of a project or technology refers to the very need for a solution, and can be achieved through clear problem definition, good project governance but also cost-benefit analysis. This paper proposes a methodology through which the costs and benefits, economic and beyond, of a security project or technology can be assessed. This methodology, though not always quantifying costs, is a key decision-making support for designers as well as a measure of the value of what is often a public good.

2. The role of **acceptability** builds on the assessment of the social and public value of a technology or project. Acceptability accounts for the crucial role of how citizens (but also staff such as engineers) consent to and perceive a technology. This accounts for context and helps to assess proportionality. Drawing on literature on technology acceptance as well as a focus group-based methodology, this paper shows the stakes of accounting for citizens' perspectives and provides a methodology for doing so.

3. **Ethics** relates to the values and moral standards guiding a project. These include fundamental rights, inclusivity, the notion of a social contract of state and citizen, trust, as well as what vision of 'security' is sought by a project or technology. Even though some of the key values at stake are included in the legal framework, social and technological forecasting are also used as methods to assess long-term externalities on society at large.

4. While **data management** does refer to the legal framework of privacy and data protection, it also encompasses much broader considerations relating to individual control and consent, methods of anonymization, and how privacy issues can be designed into technologies and projects. This methodology identifies the critical moments in data management on how a responsible approach con contribute to mitigate them or avoid them altogether (see Figure 2).

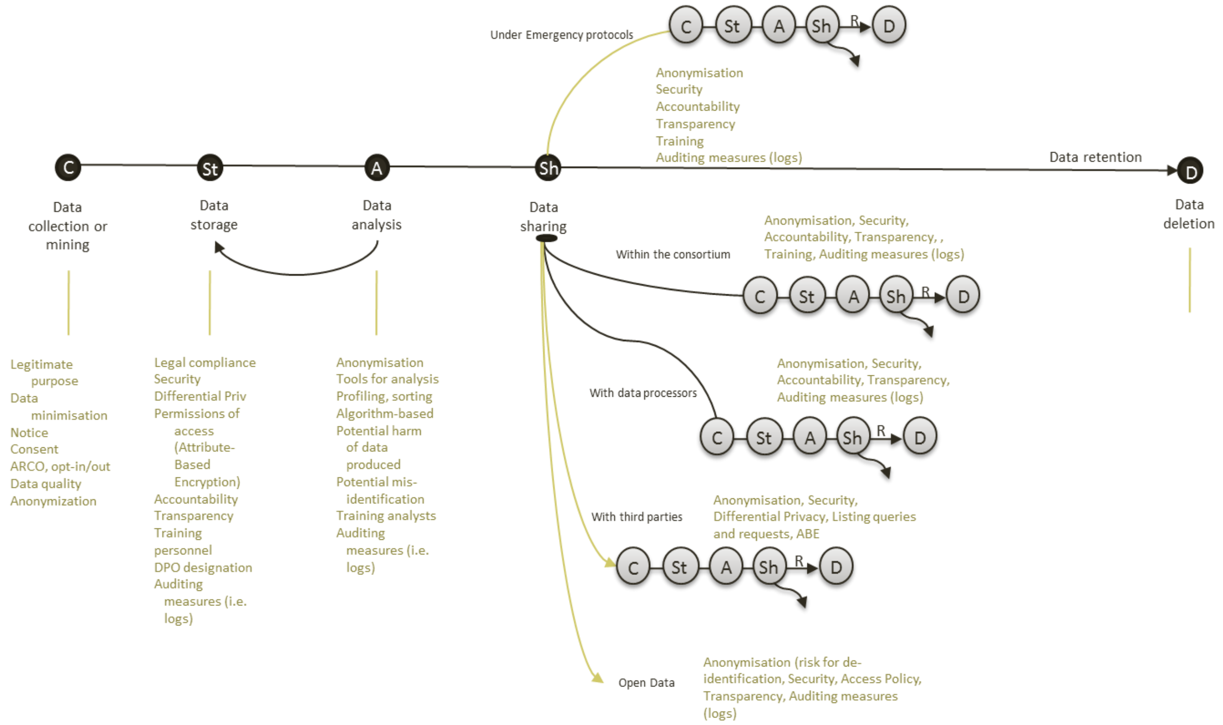
Under Emergency protocols
C
St
A
Sh
R
D
Anonymisation
Security
Accountability
Transparency
Training
Auditing measures (logs)
Data retention
C
Data collection or mining
St
Data storage
A
Data analysis
Sh
Data sharing
D
Data deletion
Legitimate purpose
Data minimisation
Notice
Consent
ARCO, opt-in/out
Data quality
Anonymization
Legal compliance
Security
Differential Priv
Permissions of access (Attribute-Based Encryption)
Accountability
Transparency
Training personnel
DPO designation
Auditing measures (i.e. logs)
Anonymisation
Tools for analysis
Profiling, sorting
Algorithm-based
Potential harm of data produced
Potential mis-identification
Training analysts
Auditing measures (i.e. logs)
Within the consortium
Anonymisation, Security, Accountability, Transparency, , Training, Auditing measures (logs)
C
St
A
Sh
R
D
With data processors
Anonymisation, Security, Accountability, Transparency, Auditing measures (logs)
C
St
A
Sh
R
D
With third parties
Anonymisation, Security, Differential Privacy, Listing queries and requests, ABE
C
St
A
Sh
R
D
Open Data
Anonymisation (risk for de-identification, Security, Access Policy, Transparency, Auditing measures (logs)

Figure 2. Key vulnerable moments in Data management and how to minimise them

Using this methodology, the paper develops the lessons learnt from implementing this approach and the specific privacy-preserving and anonymization tools and practices developed for different technologies and contexts, including biometrics, applications or crowdsourcing and participation platforms.