Using Societal Impact Assessment (SIA) to Improve Technological Development in the Field of Crime Prevention

Gemma Galdon Clavell[1,2(✉)] and Philippe M. Frowd[1]

[1] Eticas Research and Consulting, Barcelona, Spain
{gemma,philippe}@eticasconsulting.com
[2] Universitat de Barcelona, Barcelona, Spain
gemma.galdon@ub.edu

Abstract. Geographical information systems (GIS), intelligence-led policing, and automation of border controls are approaches to crime prevention heavily reliant on technology as a fix for faster data gathering and processing. This paper proposes a four-part societal impact assessment (SIA) methodology as a means of accounting for the impacts of crime prevention technologies from the standpoints of desirability, acceptability, ethics, and data management. The paper provides empirical material in two short cases on crime-mapping and automated border control.

Keywords: Societal impact · Border control · Data protection · Crime mapping · Security technologies · Technological development · Privacy

1 Introduction

A number of technologies have emerged to better allow law enforcement agencies to thwart criminal networks but also to attenuate urban insecurity. These have included geographical information systems (GIS), intelligence-based policing, monitoring of social media, the use of unmanned aerial vehicles (UAVs) and automation of immigration controls. In each of these cases, technology operates as a fix to improve data gathering, facilitate decision-making, or speed up security procedures. However, the adoption of new technologies, in order to guarantee their efficacy and to minimize their negative externalities, should be subject to a clear and comprehensive set of assessment guidelines. All too often, such technologies have led to unwanted effects: disproportionate targeting of identifiable groups, excessive costs, and more. In light of this, this paper argues for a greater attention to societal impacts in the development of crime-fighting technologies, doing do by drawing on existing practices in urban crime management through GIS as well as on the ongoing automation of border controls in Europe. The paper begins by providing a working definition of societal impact assessment (SIA) as a means of developing a four-part framework for the assessment of security technologies and projects. The primary takeaway point from this paper is that developers and operators of digital crime-fighting technologies, in order to maximize *both* effectiveness and social responsibility, should endeavour to include a holistic

L.M. Aiello and D. McFarland (Eds.): SocInfo 2014 Workshops, LNCS 8852, pp. 118–124, 2015.
DOI: 10.1007/978-3-319-15168-7_16

social impact awareness into their products and procedures. In this way, the paper provides both theoretical development as well as operational examples showcasing the potentials of a societal impact lens.

2 Societal Impact Assessment (SIA)

Societal impact assessment focuses on the potential consequences of policies, programs, projects and technologies. It is the evaluation of the risks, externalities and consequences of technologies, policies, programs, and systems. Societal impact includes the intended and unintended consequences of development, and these consequences can be changes in people's way of life; their culture; a community's cohesion and trust, stability, character, services and facilities; political systems; environment; health and wellbeing; personal and property rights and/or fears and aspirations concerning safety and future.[1]

According to the ASSERT project,

> SIA is the process of understanding, managing and responding to the societal impacts that arise from security research and the application of innovative security measures. The use of the term societal (rather than social) connotes the inclusion of anything affecting human, natural or artefactual systems, rather than just those effects that impact upon humans and their interactions. It also allows us to distinguish the process from social impact assessment […][2]

SIA's origins are multiple, and it comes from a long line of methods of assessing impacts of technologies as well as impacts on the environment. SIA can trace its proverbial 'roots' to impact assessment methods such as constructive technology assessment (CTA) as well as environmental impact assessment (EIA) and privacy impact assessment (PIA). Each of these strives to provide some form of holistic view of what a particular project, technology or program's effects (both negative and positive) might be.

The value-addition of societal impact is that it takes into account technology and design as much as social/human impacts, which allows considerations relating not only to rights and ethics questions but also to elements such as design, cost-benefit analysis and project management. SIA is therefore not only a critical tool from the sociological standpoint, but a useful approach for designers, engineers and end users to better design and implement crime-fighting technologies.

---

[1] Vanclay F.: Social Impact Assessment: International Principles. International Association for Impact Assessment, Special Publication Series no.2, 8 (2003).

[2] Barnard-Wills, D., Wadhwa, K., Wright, D.: ASSERT Project Deliverable 3.1: Societal Assessment Manual and Toolkit, 9 (2014).

So what might a framework attuned to societal impact look like? This paper proposes a four-pronged approach centred on *desirability*, *acceptability*, *ethics*, and *data management*.

2.1 Desirability

The desirability of a program refers to the very need for a solution. To think about desirability is to define the **problem** to be resolved and ensure that the design of the solution is collaborative, accounts for societal impact, and is well governed. Assessing the desirability of a project is helpful for designers as it may help to determine whether a particular **solution** is needed at all, or whether it is best to have a 'do-minimum' or 'do-nothing' solution. This can be achieved through **cost-benefit analysis** which takes into account key factors such as utility, impact and costs in an economic but also societal sense. The desirability of a security technology should also be guided by the organizational needs of the implementer, such as **staffing** which includes training and resource allocation. Personnel may need training in societal impact as well as on use of the technology chosen, and scarce resources (especially in the public sector) may be diverted for little gain. Desirability of a technology may be affected by how well it is **governed**. Assessment should include an attentiveness to accountability procedures, enforcement mechanisms, and how well best practices are formulated and applied.

2.2 Acceptability

The acceptability of a security technology builds on desirability to include public debate and consent. Acceptability is fundamentally more public-facing, and includes an emphasis on **choice**, **consent** and **control**. Technologies or programs require accountability on the part of an informed user base and broader public, and as such designers should provide adequate **information** to the public, and frequently gather the informed and voluntary **consent** of the public or intended users of a technology. Consent is an essential part of how well a technology is accepted precisely because it allows users control over their data as well as over the outcome of the technological deployment, which in its turn can impact **trust**. Acceptability of a technology or policy is also shaped by an understanding of the societal **context**, which includes overarching societal values and to what extent they might limit what users are willing to accept. Finally, **proportionality** is a key test of whether a particular technology is acceptable or not, ensuring that the effects of a solution are kept in relation to the problem it is trying to solve: for example, collection of personal data for crime mapping may be disproportionate once it begins to impact on the presumption of innocence.

2.3 Ethics

Ethics refers to the values and moral standards that guide a particular innovation or technology. Ethics are reflected in some formal documents such as those laying out **fundamental rights**, but are also composed of more intangible **values**. These are continually in flux but in democratic societies tend to include freedom of movement,

freedom of assembly, the right to free speech, freedom from discrimination, equality guarantees, and so on. Taking ethics into account necessarily means guaranteeing **inclusivity**. Inclusivity recognizes differences in accessibility, such as disability, but also imbalances in social power and access to social capital. It therefore accounts for the fact that some groups may be more affected than others and that access to services may not be equal. An ethical approach should also take into account the **precautionary principle** by which the onus is on designers, rather than the public or end users, to justify the deployment and potential risks associated with a security technology. With this onus on designers and developers comes an additional responsibility to clearly lay out the vision of **security** that is part of the technology being designed, and justify exactly what threats and being secured against, and who is being secured.

2.4 Data Management

Privacy and personal data protection is a legal and societal question. Taking into account data management compels engineers and other data managers to **follow existing law** but encompasses principles such as **minimization** and **anonymization** of data collected, as well as design techniques such as **privacy by design** (which advocates building privacy into technologies) and tools such as **privacy-enhancing technologies** (user tools for anonymity and data protection). An attentiveness to data management questions urges a careful consideration of what data is collected, from whom, for what purpose, and what rights the user has to deletion and **redress**.

3 Assessment of Existing Crime-Fighting Technologies

3.1 Crime Mapping by GIS

Police forces have increasingly sought to technologize policing tools, and GIS mapping has become an important tool for policing through a better grasp of the different layers of the very urban space of law enforcement. GIS is a compounded system made up of hardware, software and informational processes. It is designed for the gathering, management, analysis, modelling, and display of geographical data. It is primarily used for the purpose of establishing patterns, correlations to visualize often undetectable or previously unseen data.[3] For example, GIS systems can plot as well as overlay different sets of overlapping data such as urban grids, topographical maps, land use patterns and satellite imagery.

Technologies for GIS mapping of crime have been developed in order to make policing more *efficient*. Some of the earliest GIS systems were deployed before the digital age by police departments in the United States, with the St. Louis police using this technology to improve the efficiency of its patrol routes based on the SYMAP punch card system developed at Harvard University. In the 1990s, the New York Police Department began to explicitly deploy systems to make policing a strategic and intelligence-led operation based on crime statistics, beginning with COMPSTAT

[3] Galdon Clavell, G., Pybus Oliveras, M.: Crisis Economics y Gestion de la Inseguridad Ciudadana: Los Mapas de Delincuencia. Revista Catalana de Seguretat Publica 24, 79-105 (2011).

(Computer Statistics). With the development of complex ICTs, a range of GIS tools now includes CrimeStat, CrimeWiew, Spatian Analyst, HotSpot Detective Vertical Mapper, SpaceSat, and many more. The ClearMap system deployed by the Chicago Police not only relies on statistics but also on geolocation of crime through GPS coordinates and is integrated with databases of sex offenders. The development of GIS-based crime mapping is inseparable from a faith whereby investments in technology, irrespective of budgetary situation, are considered good investments. In the case of crime mapping, the technological possibilities of mapping technology have actively shaped policing tactics. What could a lens attuned to societal impact add to the study of police mapping practices? What kinds of new questions could be raised in terms of desirability, acceptability, ethics, and data management? These are reflected in some of the sample assessment questions provided in Table 1, below.

Table 1. Potential questions to be asked of GIS-based crime mapping

Desirability • Has there been any cost-benefit analysis carried out in relation to the purchase of GIS equipment? • What alternative options exist to better combat crime by geographic area, and how are they to be weighted? • Has implementation been accounted for, including staffing and training?	**Acceptability** • To what extent are the public aware of, and specifically consenting to, the use of GIS mapping? • How have the public been informed of the use of GIS information for policing? • At the institutional level, have personnel been consulted about their perspectives on GIS mapping techniques?
Ethics • How does the use of crime mapping potentially exclude identifiable or vulnerable groups? • What measures are in place to ensure that the use of GIS mapping remains limited to its original mandate? • Have key values such as freedom of movement been assessed in light of the use of GPS systems? • Could crime mapping lead to hot-spot policing and a disproportionate police presence in vulnerable areas?	**Data management** • Are those who have police contact (e.g. arrest) aware of the collection of their data? • How is data kept secure, and who has access to the databases the system connects to? Are searches of the database logged? • Have privacy by design principles been considered in the design of the GIS system itself?

Table 2. Potential assessment questions for automated border control

Desirability	**Acceptability**
• Do ABC gates provide any cost savings for their operators, or time savings for their users, and in what relation do these benefits sit in relation to the economic cost of these systems? • What have countries outside the EU tended to adopt for automation of border control, and how can this experience shape the EU's own deployment? • How can gate designers and engineers be trained on societal impact in a way that is meaningful and can be translated into their professional routines?	• How do ABC systems conform to existing law (such as the Schengen Borders Code), particularly in relation to their automation of border procedures? • What is the public perception of ABC gates, and how has this been measured? • What measures are in place to inform travellers of the presence of ABC gates and ensure that they use them with freely given consent? • What data is published about the efficacy of ABC gates and is it publicly available?
Ethics	**Data management**
• Is the use of biometrics for border control potentially encouraging the broader use of biometrics throughout society? • What provisions have been made in the physical and human interface design of the gates to ensure that they are accessible to persons with disabilities? • What ideal of security is put forth by these gates, and do they contribute to an ideal of borders as primarily security-related spaces? • Is the autonomy of travellers protected by the ability to opt-out or use fallback measures of equal quality? • To what degree does automation potentially remove agency from the traveller or lead to inequality?	• What transfers of biometric information are put in place? • What are the rates of false rejection in the biometric matching? • Is biometric data stored locally, or on an off-site database, and is it deleted immediately after each traveller passes? • What steps have been taken to avoid unnecessary polling of databases?

3.2 Automation of Border Control

Several European states have, over the last decade, attempted to automate elements of their border management processes. This has included but not been limited to passport/ID control, with visa issuance and entry/exit tracking increasingly automated and interlinked. Sweden has automated elements of its visa issuance and verification system and interlinked it with its diplomatic missions abroad, while states such as France and Germany provide automated border control (ABC) for biometric passport holders at some main airports. A majority of states in Europe now have some form of automation of border procedures. Automation of border control is partly an issue of convenience, as it theoretically speeds up border crossing. However, ABC also serves to prevent identity fraud and to stifle criminal networks proliferation of forged documents. The adoption of biometric travel documents, called for by international norms (like the International Civil Aviation Organization's Doc 9303) and by EU directives (such as Council Regulation EC 2252/2004) specifically aims to combat this threat and these documents are the backbone of border control automation.

In the pursuit of a more harmonized and societally-conscious solution, at least for states participating in all aspects of the Schengen Agreement, the EU has funded a number of studies, including two large projects–FASTPASS and ABC4EU–under its Seventh Framework Programme (FP7) research funding. These projects are oriented towards assessment of the legal possibilities of automation of border control and, due to their public-private nature, are building and deploying prototype units to test elements of border control automation, from document verification to biometric matching to user interface. In each project, but particularly in ABC4EU, there has been an opportunity to introduce an awareness of societal impact from the beginning of the development process, to ensure that the designers of the gates are trained on societal impact and that the final product is reflective of the broad societal consensus. Some of the questions asked of ABC gates are included in Table 2, below.

4 Conclusion

This paper has explained some of the essentials of SIA and set out a four-pronged framework for assessment of security technologies. It has then used two examples of current crime-fighting tools to suggest some beneficial applications of such an approach. Going forward, SIA can prove itself to be a fruitful lens not only for critics of similar security technologies, but also for their designers. The SIA approach ensures that fundamental rights are respected, that societal impacts (and project impacts) are considered, and that technologies are able to carry out their security functions without compromising the type of society in which we wish to live.

References

1. Barnard-Wills, D., Wadhwa, K., Wright, D.: ASSERT Project Deliverable 3.1: Societal Assessment Manual and Toolkit, 9 (2014)
2. Clavell, G.G., Oliveras, P.M.: Crisis Economics y Gestion de la Inseguridad Ciudadana: Los Mapas de Delincuencia. Revista Catalana de Seguretat Publica **24**, 79–105 (2011)
3. Vanclay, F.: Social Impact Assessment: International Principles. International Association for Impact Assessment, Special Publication Series no. 2, 8 (2003)