Go and stop them (but don't tell anyone that an algorithm said to)!

Monitoring Public Life in Germany

MiT8 conference paper, April/May 2013

Stephan G. Humer[1]

Thomas Petzold[2]

CCTV, video surveillance and public monitoring are ubiquitous in Germany. There are not as many cameras and surveillance systems as in the UK or in cities like New York. However, conventional video surveillance is nothing new, albeit it still causes public controversy. Germany is a country with very high data protection standards, many well-established regulatory data protection bodies and a very state-skeptical public that gains many of its opinions from a traditional and distinct community of also well-established media corporations, many of them quite opulently funded by the public itself.

Public discussions about risks and opportunities of video surveillance have traditionally been driven by both politicians, interest groups and technology organizations who demand an increased use of video surveillance, for example to prevent terrorist attacks, as well as politicians and interest groups who object to these proposals, for example on ethical grounds. With the augmentation of digitized, computational technology that diffuses into people's social practices, habits and routines, digitized surveillance as a public issue gains renewed momentum as it alters the rules, structures and methods of a previously non-digital phenomenon. And like any revolution, Digitization has a lot of inherent laws and autonomous rules, or simply said: it changes our life-world a lot, especially through video surveillance. Two things are important consequences of this development:

a) Digitization is much more than just Technology
b) Digitization shows us rules, structures and methods that offer us a new view on *non-digital* phenomena.

These two aspects combined sum up to an applied Sociology of the Internet which is the basis for the framework described in this paper: when it's possible to get better results about a flu epidemic

---

[1] Research Director, Berlin University of the Arts (UdK), humer@udk-berlin.de
[2] Professor of Media Management, HMKW - University of Applied Sciences for Media, Communication and Business Administration, Berlin

through analyzing Tweets instead of calling medical practices in a specific region, then it's time to switch to the digital method.

In this paper, we propose an applied framework that helps us analyzing public monitoring in such a context of totally new digital influences and inherent laws. The conceptual framework presented here is "Sociality by Design". It offers a clear cut By Design Approach just like Privacy By Design, but uniting the three main elements Privacy and Technological Impact Assessment (PIA/TIA), Acceptance Research together with Acceptability Findings and the crucial relation of people and technology. This framework supports fast and efficient solutions e.g. by focusing on the discovery of relevant discourses performed by the public regarding video surveillance. It reveals human aspects and thoughts behind media discussions, connects it to current law, and offers a built-in solution for the implementation of new results and methods. Its core aspects are a structuralist toolbox approach based on Michel Foucaults discourse analysis, a tech screening down to 0 and 1 (without any aloofness towards code) and the equilibration of Technology and Society. Such a By Design Approach achieves the following:

a) It helps people dealing with digital surveillance phenomena, because a clear Open Standard Structure frames phenomena and events that lack a classic (analog) coping strategy

b) It offers more than just a Privacy or Technological Impact Assessment (PIA/TIA) and classic Acceptance Research (which quite often lacks Acceptability findings and – even worse – a participation of aggrieved parties) because it adds the crucial relation between "man and machine" which is still a quite large blind spot in socio-scientific research with a lot of work to do and definitely powered by the finding that often enough it is impossible to derive digital strategies and methods from analog experiences. ("Better" PIAs already have this insight and try to "assess the impacts in terms broader than those of legal compliance" (Warren, A., et. al. (2008). Privacy Impact Assessments: International experience as a basis for UK Guidance. Computer Law and Security. pp. 233-242. Quoted by Cavoukian, A. http://privacybydesign.ca/content/uploads/2012/06/pbd-drones.pdf, p.16))

Ann Cavoukian, inventor of Privacy by Design, states that "PbD represents a significant shift from traditional approaches to protecting privacy, which focus on setting out minimum standards for information management practices, and providing remedies for privacy breaches after-the-fact. PbD requires an evolution in the way that organizations think about privacy – moving from a reactive mode to a proactive one. Similarly, enshrining PbD in regulatory instruments, voluntary codes, and best practices requires an evolution in how policy and law makers approach privacy rule-making"

(Cavoukian, p. 17) This is an example for the necessity to focus on more integrated solutions and PbD seems to be the best paradigm for that.

This paper looks at the specific example of multi-biometric video data analysis for public places in Germany. It examines this by inspecting involved actor's attitudes about newly employed computational technology, their capacities to use these technologies (micro - individual) for daily crime detection in general (meso - organisational) as well as the impact that regulation of new surveillance technologies in Germany has (macro – society). Analyzing these conditions with the proposed framework is expected to help develop a stable, sustainable and common ground across involved communities – ranging from tech developers to regulatory instances to the concerned public. Driven by large-scale availability of new technologies and an increase of hardware networking, software possibilities are adding to legal and public monitoring discussions. Learning algorithms, for example, are used to operate smart cameras that (help) identify people, gestures and movements in public places. We are now observing a leap from *conventional* to *intelligent* video surveillance, but we know that there still is a deficit on adequate social norms and coping strategies. There is, for example, no regular Police training course regarding (digital) video analysis in Germany, so every local and state police agency has the power to perform own seminars and trainings, without the necessity of focusing on specific Frameworks or up-to-date research. This corresponds with judicial praxis that still struggles with intelligent video analysis as evidence in court. The multi-biometric video data project which is the test case for Sociality by Design focuses on an intelligent analysis of existing video material, because one major problem of today's video surveillance projects is that there is a lot of (low quality) video data, but no time and/or no personnel for a reliable analysis that's fast and good enough for compliant manhunt purposes or other emergencies. Existing solutions that are already on the market focus primarily on efficient compositions of visualizations and hardly on algorithmic image content analyses. Intelligent video analyses should focus on a supportive role for police and other agencies to fulfill their needs, but without forgetting the expectations of lawmakers and the public, so this is where Sociality by Design comes into play. And because of Digitality's inherent laws there is even more to consider: examples like manhunts based on distributed police mug shots nowadays show that data flows *bidirectional* which is a new challenge for police work. The public can support the police with own pictures showing suspects on a crime scene, being helpful in this case, but also destructive by ignoring privacy rights of possibly innocent people in the heat of the moment. This Big Data aspect has to be connected with the video data already used, but again in a way that builds a common denominator for all parties involved.

Digitality needs to be designed, not feared. Following a By Design approach means that SbD is not a single issue, but enmeshed with other By Design Strategies like Privacy by Design, Legality by Design

etc. It also builds up a basis for defending freedom and privacy by confronting rather aggressive ideas like "Surveillance by Design". SbD *empowers people*, supports Digital Literacy efforts and offers connections and starting points for future developments and phenomena. The whole project is still work in progress, but concrete examples can already be delivered by taking a closer look on the mass video data project socio-scientific methods:

- media analysis (online discourses about video surveillance)
- observation (of R&D processes and police procedures regarding video surveillance)
- interviews (with police officers and video surveillance staff about their daily routine and future perspectives regarding video surveillance)

It examines if and how large-scale monitoring data and learning algorithms are successfully connected and used in local police procedures – ranging from classic public place surveillance for the prevention of violence to smart face and gesture detection for manhunt purposes – and how one can find out what the public thinks about these different solutions. The main problem is that intelligent video surveillance has no precursor that can be used as an orientation, so it seems to be even more necessary to have a stable framework that assembles all important aspects of Digitality to a clear picture and a stable ground for applied solutions. Sociality by Design should fulfill this task and it has to be discussed how the methods and structures used in this Framework can help building a common denominator working for all three main areas of digital influence: technology, law and society.