Surveillance in the Context of Security and Profit – The Case of „non-volunteered“ Geographic Information

Paul WEISER[1] und Amin ABDALLA[1]

[1]Department für Geodäsie und Geoinformation · Forschungsgruppe Geoinformation · Technische Universität Wien · Gusshausstr. 27-29 · 1040 Wien
E-Mail: {weiser, abdalla}@geoinfo.tuwien.ac.at

1 Introduction

In the past, the access to digital geographic information (GI) was both limited and associated with high costs. Most of it was owned and produced by public authorities and private companies. Today, however, GI is increasingly collected and produced by ordinary citizens, often publicly available at no cost. This process has become known as Volunteered Geographic Information (VGI).

In contrast to VGI, where people use mobile sensors to collect data actively and by choice, an increasing amount of GI is collected involuntary, i.e., without the knowledge and/or consent of the people involved. For example, in 2011 it was revealed that UMTS enabled mobile devices by Apple Inc. store locational data as well as associated time-stamps of their users and share this information with a central database[1]. Together with in- and outgoing calls, text messages, and additional information (e.g., from social networks) it is possible to create a detailed profile of a person's activities in space and time[2]. The growing interest in personal spatio-temporal data is not limited to companies alone. In February 2011, German police collected 500 000 cell phone data records (locational data, in- and outgoing calls, text messages) from people attending an anti-nazi demonstration in Dresden, without having the legal permission to do so. In both examples, people were not aware that their locations had been collected, stored, and subject to further analysis.

While both companies and authorities keep insisting that the collection and storage of locational data is to our benefit, either to make our lives easier or to improve our security, the potential for abuse can hardly be ignored. The ubiquitous surveillance of citizens as envisioned in George Orwell’s novel “1984” has become, at least technically, feasible.

During our research, we have gained the impression that this issue has, at least so far, found not much attention inside the GI research community. Ethical questions, however, do arise if technologies and methods developed by GI researchers are used in this context. At the same time, we noticed that many security and surveillance related research projects funded by the European Union (EU) are actively supported by universities and research institutions. Security and surveillance are “going spatial” and this trend is of interest to research

[1] http://en.wikinews.org/wiki/Apple_collecting_location_data_from_iPhone,_iPad

[2] http://www.zeit.de/datenschutz/malte-spitz-vorratsdaten

institutions and companies alike. As a result, we present some EU research projects and applications that either actively research and develop surveillance methods or use them as a core feature in their commercial products.

Contrary to popular belief, it is not entirely certain that the technologies proposed to improve our security have the desired effects. In general, an evaluation and discussion on the ethics of surveillance methods, by the research community itself, is crucial because we believe this is an effective way to "watch the watchmen" (WEISER & ABDALLA, 2011). We present studies investigating the impact of camera surveillance on crime. Because this prototypical form of surveillance has long been in place, a considerable amount of data is available to allow for an evaluation.

We criticize that the research community does not sufficiently address ethical issues of geographic information in the context of surveillance. The main goal of this paper is to start a discussion on this issue.

2 Non-volunteered Geographic Information (NVGI)

The term Volunteered Geographic Information (GOODCHILD 2006) has become popular to describe "the widespread engagement of large numbers of private citizens, often with little [...] formal qualifications, in the creation of geographic information“. Goodchild also emphasizes the fact that they do this "almost always voluntary".

In contrast to VGI we define the term "non-volunteered" Geographic Information (NVGI), as the creation of personal spatio-temporal geographic information, without the knowledge or consent of the person involved in the data collection task. Information of this kind results from sensors that are either carried by the person himself (e.g., mobile phone) or installed at fixed locations (e.g., surveillance cameras). They are pervasive in nature and can hardly be avoided due to their ubiquitous or disguised nature.

The next section discusses examples of research projects and commercial applications that contribute to the creation of NVGI.

3 Surveillance in the Context of Security and Profit

LYON (2007), defines surveillance as the "focused, systematic, and routine attention to personal detail for the purposes of influence, management, protection, or direction". It follows that privacy and surveillance are mutually exclusive terms. Arguments in favor of surveillance often justify the loss of privacy with certain benefits, e.g., improved security. What struck the authors most while examining the examples presented in this section is that the collection of personal spatial information, often in combination with behavioral pattern detection, were such prominent terms.

3.1 Surveillance as a topic in EU funded research projects

It seems that in times of state budget-cuts and increased economic pressure, securing external funding has become an essential pillar for many research institutes. External funding often comes with particular interests from the financiers. Yet, the goal of this paper is not to spawn a discussion on the principles of good scientific practice and independent research. We believe, however, it is at least important to discuss and question some of the goals these projects aim at.

One of the largest financier of research projects in Europe is the EU. Several framework programs (FPs) offered by the EU provide a main source for external funding in research. The current FP7 (2007 - 2013) runs over the course of seven years and has an overall budget of 50 521 million Euro.[3] There are ten high level themes proposed in the program, including Health, Energy, and Environment (among others). The "Security" theme has a budget of 1.4 billion Euros which is relatively small in comparison to others but still double the budget of "Socio-economic Sciences and the Humanities" (0.6 billion). In general, companies or universities, can propose research projects related to one of the included topics for each theme to secure external funding.

Looking through the current security-related projects publicly available on the web we found 11 projects that fall into the Security category, 8 of which are presented in Table 1. Based on their project descriptions, we got the impression that they are mainly related to surveillance of individuals, and as a consequence, pose a potential threat to the right on privacy. One of the projects with the second largest budget (INDECT) has even led to EU parliamentary questions doubting the value of the project and its compatibility with privacy rights[4].

It is interesting to note that each of these projects has at least one project partner that is either a research institute or a university. INDECT, for example, is actively supported by a total of 8 universities. The project's objectives as stated in CORDIS (Community Research and Development Information Service) include the following: "[...] construction of agents assigned to continuous and automatic monitoring of public resources such as: web sites, discussion forums, UseNet groups, file servers, p2p networks as well as individual computer systems, building an Internet based intelligence gathering system, both active and passive, and demonstrating its efficiency in a measurable way."

As mentioned before, the contribution of such systems to the improvement of our security is at best unclear. This is largely due to no or weak evaluation on their effectiveness. Also, ethical considerations (privacy, total surveillance) are often addressed by the public but hardly by the project partners themselves.

[3] http://cordis.europa.eu/fp7/budget_en.html

[4] See for example http://tinyurl.com/EU-Parliamentary-Questions

Table 1: Some EU funded security and surveillance related research projects (adapted from http://cordis.europe.eu)

Name	**Project Description (Excerpt)**	**Funding (€)**	**# Universities Involved**
Hybrid Enhanced Money Laundering Intelligence, Investigation, Incrimination and Alerts **(HEMOLIA)**	[An] "intelligent […] alert and investigation system […]makes extensive use of modern society's huge telecom data source"	2,9 m	1
Intelligent information system supporting observation, searching and detection for security of citizens in urban environment **(INDECT)**	"the registration and exchange of operational data, acquisition of multimedia content, intelligent processing of all information and automatic detection of threats and recognition of abnormal behaviour or violence"	10,9 m	8
PRedictive reasOning and multi-source fusion empowering AntiCipation of attacks and Terrorist actions In Urban EnVironmEnts **(PROACTIVE)**	[…] "multi sensor fusion and intelligent reasoning framework […]prediction, detection, understanding and efficient response to terrorist interests, goals and courses of actions"	3,3 m	2
Automatic Detection of Abnormal Behaviour and Threats in crowded Spaces **(ADABTS)**	[…] "the automatic detection of abnormal human behaviour."	3,2 m	1
Multi-Modal Situation Assessment & Analytics Platform **(MOSAIC)**	[…] "data intelligence capture and analytics including video and text collaterals etc. […] "decision support for automated detection, recognition, geo-location and mapping"	2,6 m	1
Suspicious and abnormal behaviour monitoring using a network of cameras & sensors for situation awareness enhancement **(SAMURAI)**	[…] "develop and integrate an innovative intelligent surveillance system for robust monitoring of both inside and surrounding areas of a critical public infrastructure site"	2,4 m	1
Total Airport Security System **(TASS)**	[…] "surveillance system, aimed at creating an entire airport security monitoring solution providing real-time accurate situational awareness"	8,9 m	2
Surveillance of unattended baggage and the identification and tracking of the owner **(SUBITO)**	[…] "automated real time detection of abandoned luggage or goods and the fast identification of the individual who left them and their subsequent path"	2,5 m	2

3.2 Surveillance in Applications

Many of the research projects described in the previous section are still in a prototypical stage. There are cases, however, where similar systems are already deployed and in use, all of which either collect, analyze, or store personal location data. The following, not exclusive list, mentions a few:

- In Minneapolis, USA, police is logging car movements by tracking license plates from camera surveillance data[5]. A similar system is used by British police forces to monitor the behavior of people living in two particular areas of Birmingham[6]. The fact that these areas are predominantly inhabited by an ethnic minority gives rise to ethical questions.

- Another example is the use of phone data by German police for criminal investigations. It was revealed that German police in Berlin requested 6.6 million phone records (including locational data) for a period of 3 years (2009-12) with the goal to investigate cases of arson. In 116 cases police could get useful information[7]. This figure seems quite low if one considers the huge amount of data collected. The example stands for the concerning development of company owned private data exploited by state institutions.

- Some schools have started adopting surveillance technologies to track their students. The main goal according to O'CONNOR (2012) from RFID Journal is to "help the college ensure that it deploys adequate resources throughout its buildings". Here RFID tags are used to monitor attendance and location of students on campus.

While afore mentioned examples have, at least officially, a benefit for the society, e.g., increased security and better crime prevention, some methods used by private companies are of questionable value.

- The Spanish telecommunications company “Telefonica” aims to exploit its customer’s locational and demographic data with the goal to sell this to marketing companies[8].

- Two British car insurance companies, announced that they are going to introduce insurance premiums for their customers based on a new statistical index. The basis

[5] http://arstechnica.com/tech-policy/2012/12/found-secret-location-of-minneapolis-police-license-plate-readers/

[6] http://www.guardian.co.uk/uk/2010/jun/04/birmingham-surveillance-cameras-muslim-community

[7] http://www.spiegel.de/netzwelt/netzpolitik/neue-zahlen-funkzellenabfrage-in-berlin-2009-bis-juli-2012-a-852325.html

[8] http://www.tagesschau.de/wirtschaft/telefonica106.html

for the index are the customer's demographic data and the driving behavior recorded by GPS devices.[9] [10]

Some afore mentioned examples illustrate the connection between research on surveillance and the use of its results in other domains. In most cases, the use of personal locational data stands out as the prominent term. In the case of companies surveillance technologies are simply used to maximize profit. Unfortunately, this comes at the cost of privacy and with questionable value for the customer. Most people are not even aware of the fact that their personal data is tracked, stored, analyzed, or sold. If people knew they could decide whether they want to allow companies to use their data (opt-out).

4. Evaluating the Effects of Surveillance on Security

In this section, we present empirical evidence based on cases of camera surveillance in the UK showing that there is little causality between increasing surveillance and improving security. The widespread use of cameras as a surveillance method is often justified because it supposedly allows for better crime detection, increases crime prevention, and improves the overall feeling of safety among citizens.

We investigate these popular claims by summarizing findings from studies done in the UK evaluating the effectiveness of camera surveillance. We limit ourselves to studies in the UK because the amount of available data from Germany is either too small or the studies do not meet the criteria allowing for a scientific analysis (GLATZNER 2006).

4.1 The situation in the UK

As of 2011, there are an estimated total of 1.85 million surveillance cameras in the UK (GERRARD & THOMPSON, 2011). On average, every citizen of a major city in the UK is filmed 300 times per day (GRAS, 2003). Given the high numbers and associated costs a regular evaluation seems logical. This, however, is not really the case. According to a study by the HOUSE OF LORDS (1998), only 0.02 per cent of the public budget available on camera surveillance is spent on evaluating the effectiveness.

In the following we present the findings of two independent studies undertaken in the UK to evaluate the effectiveness of camera surveillance.

4.2 Study I

WELSH & FARRINGTON (2002) reviewed the effects of camera surveillance on crime prevention in three different settings (city center, public housing, transportation) of 22 study evaluations in the UK and North America. A meta-analysis of 18 of the 22 reviewed evaluations was carried out. Welsh and Farrington concluded that 9 studies showed evidence of a

[9] http://www.computerworlduk.com/news/it-business/3358014/car-insurance-firm-uses-analytics-set-premiums

[10] http://www.computerworlduk.com/news/mobile-wireless/3375828/aviva-measures-safer-driver-premiums-via-smartphones

desirable effect of camera surveillance on crime while the other half did not. Violent crimes were not affected while the authors could find a desirable effect on vehicle theft. Mixed results were presented for the effectiveness across the different settings. In the city center and public housing settings, evidence showed that the reduction in crime was negligible. The public transportation setting showed mixed effects. The authors criticized that most studies did not study diffusion of benefits or displacement. The effects of other measurements in place could not be analyzed, because none of the data that would have allowed this was available.

4.2 Study II

In a more recent study by GILLS AND SPRIGGS (2005) 13 camera surveillance projects throughout the UK were investigated. The authors noted in accordance with study I that camera surveillance appears to have a varying effect on different types of crimes. Spontaneous offenses, e.g., violence did not decrease while more planned offenses, e.g. vehicle crime did decrease. The authors found little evidence that the fear of crime was reduced due to the presence of CCTV. Also, authors stated that in all but one area CCTV systems failed to reduce crime. Acknowledging the complexity of the topic, GILLS AND SPRIGGS (ibid.) concluded that CCTV cannot achieve the objectives it was set up to.

5. Conclusion

This article aimed at sparking a critical discussion on current developments in surveillance research and its applications, both of which are increasingly making use of personal locational data. In general, we found that there is little research on the evaluation of the effectiveness of surveillance as a security measure. The studies related to camera surveillance suggested that there is only a marginal crime reduction, mostly for property related crimes. Often, other potentially measurable effects (e.g., increased presence of police) were not included in the studies. Therefore, it is difficult to attribute the changes in crime rates to camera surveillance alone. We believe it is time to think about measures that help to monitor the effectiveness of surveillance in terms of their goals. When the goal of a Million Euro system is to improve security, it is crucial to know whether its initial purpose is met or not. The argument that research on improving existing surveillance methods will achieve the desired effects does not justify the loss of privacy and a ubiquitous surveillance as a result.

Besides the sometimes questionable argumentation based on improving security, we listed several examples where surveillance is used to achieve completely different goals, i.e., for profit maximization. As a consequence, we defined the term „non-volunteered“ Geographic Information (NVGI) to draw attention to the fact that increasing amounts of personal spatio-temporal data are produced without our knowledge and / or consent.

Because most people do not want to abstain from location based services we have to think of better ways how our privacy can be guaranteed. One possible method is to allow the user to store and synchronize their personal data locally as opposed to using “cloud” storage. Services can then access the data stored on a mobile device (e.g. phone) but do not have to

send personal data back to the server. For example, many alternative database concepts (cf. NoSQL) have strong selective offline synchronizing capabilities while at the same time putting their main focus on Web based applications. Whether this approach could be used to improve personal data security is a direction for further research.

Examining the EU projects presented in this work revealed that security research is mainly concerned with gathering and processing information about individuals but does not consider ethical issues. In the late 90ies, articles, labeled under the term "critical geography", started to address similar issues that had not been discussed before. For example, DOBSON (1998) was the first to ask if "GIS is a privacy threat?" Likewise, CRAMPTON (1995) asked emerging questions related to ethics of GIS. DOBSON & FISHER (2003), early GIS pioneers, warned the research community from becoming advocates of what they called "Geoslavery".

Due to recent GIS developments (big data, VGI, social networks) and considering that 10 years have passed since the last serious discussions on privacy and the ethics of GIS, we would embrace a new discussion of these issues. This is especially needed inside the German speaking research community on GIS.

References

CRAMPTON J. (1995), THE ETHICS OF GIS? IN: CARTOGRAPHY AND GEOGRAPHIC INFORMATION SCIENCE, 22 (1), 84-89.

DOBSON J.E. (1998), IS GIS A PRIVACY THREAT? IN: GIS WORLD, 11 (7).

DOBSON J.E. & FISHER P.F. (2003), GEOSLAVERY. IN IEEE TECHNOLOGY AND SOCIETY MAGAZINE, SPRING 2003.

GERRARD G. & THOMPSON R. (2011). HOW MANY CAMERAS ARE THERE IN THE UK, CCTVIMAGE, WINTER 2011.

GILL, M. & SPRIGGS A. (2005), ASSESSING THE IMPACT OF CCTV, HOME OFFICE RESEARCH STUDY 292.

GLATZNER F. (2006), DIE STAATLICHE VIDEOÜBERWACHUNG DES ÖFFENTLICHEN RAUMS ALS INSTRUMENT DER KRIMINALITÄTSBEKÄMPFUNG – SPIELRÄUME UND GRENZEN, MAGISTERARBEIT. UNIVERSITÄT MÜNSTER, 2006.

GOODCHILD M.F. (2007), CITIZENS AS SENSORS: THE WORLD OF VOLUNTEERED GEOGRAPHY. IN GEOJOURNAL, 69 (4), 211-221.

GRAS M. (2003), KRIMINALPRÄVENTION DURCH VIDEOÜBERWACHUNG – GEGENWART IN GROSSBRITANNIEN – ZUKUNFT IN DEUTSCHLAND? NOMOS-VERL.-GES, BADEN BADEN.

HOUSE OF LORDS (1998), DIGITAL IMAGES AS EVIDENCE, SCIENCE AND TECHNOLOGY - FIFTH REPORT, 1998.

LYON D. (2007), SURVEILLANCE STUIDES – AN OVERVIEW, POLITY PRESS, CAMBRIDGE, 2007.

O'CONNOR M.J. (2012). West Cheshire College Tracks Whereabouts of Students, Staff. Available online via: http://www.rfidjournal.com/article/view/9476.

WEISER P & ABDALLA A. (2011), QUIS CUSTODIET CUSTODES - CROWD SOURCING ALS NOTWENDIGES WERKZEUG ZUR ÜBERWACHUNG DERER DIE UNS ÜBERWACHEN? AGIT - SYMPOSIUM FÜR ANGEWANDTE GEOINFORMATIK 2011, SALZBURG.

WELSH, B.C. & FARRINGTON D.P. (2002), CRIME PREVENTION EFFECTS OF CLOSED CIRCUIT TELEVISION: A SYSTEMATIC REVIEW. HOME OFFICE RESEARCH STUDY 252