Google Street View and Privacy

Some thoughts from a philosophical and engineering point of view

Oliver Siemoneit, Christoph Hubig
Institute of Philosophy, Chair for the Philosophy of Science and Technology
University of Stuttgart
Seidenstraße 36
70174 Stuttgart, Germany
{firstname.lastname}@philo.uni-stuttgart.de

Martin Kada, Michael Peter, Dieter Fritsch
Institute for Photogrammetry
University of Stuttgart
Geschwister-Scholl-Straße 24D
70174 Stuttgart, Germany
{firstname.lastname}@ifp.uni-stuttgart.de

ABSTRACT
The Google Street View technology has proven to be highly controversial. Especially in a lot of European countries – where privacy and data protection laws are far stricter than e.g. in the United States – the launch of Street View has caused many residents and citizens to issues complaints to government officials about the project thereby claiming that it is a massive intrusion upon privacy and thus a violation of existing data privacy laws. It is the aim of this paper to contribute to a better understanding of this technology and its problems by discussing it from a philosophical and engineering point of view. Existing methods for preserving privacy are criticized. Improved methods are proposed thereby also showing that Google Street View could be regarded as a kind of interstage product which should have never reached the public.

Keywords
Ethics, privacy, privacy-enhancing technologies, geospatial information systems, city models, street views.

INTRODUCTION
Technological developments usually come forth with a vast amount of new opportunities. But at the same time, technological innovations are also prone to novel, unknown problems and threats – for its latter users and/or society in general. It is the unavoidable, janus-faced nature of technology, which has also recently drawn a lot of attention to *geospatial information systems* and services. Especially in a lot of European countries – where privacy and data protection laws are far stricter than in the United States – some early kind of geospatial information system has proven to be highly controversial. The launch of *Google Street View* has caused many citizens to issue complaints to government officials about the project thereby claiming that it is a massive intrusion upon privacy and thus a violation of existing data privacy laws (see e.g. Spiegel Online International 2008). In this quite emotional, heated and sometimes even irrational debate, it could be regarded as the job of the sciences, to pick up the raised questions, to think about them, to analyze and to restructure them in joint, interdisciplinary research and finally to think of adequate solutions. It is exactly the aim of this paper, to make such a basic contribution to this debate and to shed some light on fundamental questions. Therefore, to start with, Section 2 "Privacy and its importance" elaborates on what privacy is and which value it has for (western,) liberal, egalitarian, and democratic societies. Section 3 "Privacy issues with Google Street View" builds a basic framework so as to be able to identify and to analyze different privacy intrusions. Section 4 "Possibilities and limitations of privacy-preserving abstraction and obfuscation techniques" discusses different privacy-enhancing technologies, mainly Google's pixelating-out-approach and its weaknesses. By contrast, different privacy-enabling methods and techniques already known from the construction of 3D city models are depicted thereby showing that Street View could be regarded as some kind of interstage product which should have never reached the public.

AP-CAP 2009, October 1–2, 2009, Tokyo, Japan.

PRIVACY AND ITS IMPORTANCE
Privacy and the right of privacy is central for all western, liberal, egalitarian, and democratic societies. According to the literature, three different dimensions of privacy could be distinguished: decisional privacy, informational privacy and local privacy (Tavani 2008; Rössler 2006; Rössler 2004).

Decisional privacy (sometimes also referred to as psychological or mental privacy) is the independence of a person in making certain kinds of important decisions. Decisional privacy concerns therefore first and foremost mainly basic decisions of a person about who he wants to be and how he wants to live. Decisional privacy is the core of one's personal freedom and the possibility to form one's own authentic identity. It is also the core of political freedom in the form of the absence of interferences with the sovereignty (negative freedom as "freedom from") and the assistance in fulfilling one's own potentials (positive freedom as "freedom to").

By contrast, *informational privacy* deals with the fact that a person wants to be in control of personal information about intimacies of his life. In this clearly information-based or knowledge-based conception of privacy, privacy intrusions are defined therefore as situations in which personal information is collected or disseminated without consent of the person who is topic of the information. Informational privacy is crucial for regulating personal relationships and establishing different social roles one plays in society: “If everyone knew everything about everyone else, differentiated relations and self-presentation would no longer be possible, nor would autonomy and the freedom to determine one’s own life” (Rössler 2006, p. 705).

However purely information-based conceptions of privacy are clearly flawed: There are also other privacy violations, which are not of mental or cognitive nature but of a physical one. *Local privacy* is the right of a person to restrict physical access of others to his body, his personal belongings and his home. Local privacy assures a sphere of non-intervention, a protected, secured, private place or shelter and thus corresponds well with the famous definition of Warren and Brandeis of the right of privacy as the right to be left alone (Warren and Brandeis 1890).

To conclude, one could say with Schoeman, that “a person has privacy to the extent that others have limited access to information about him, limited access to the intimacies of his life, or limited access to his thoughts or his body” (Schoeman 1984, p. 3). The right of privacy is then the right of a person to be protected against intrusions (*negative form of privacy* as being free from) and to be able to control cognitive or physical access to his personal things and affairs (*positive form of privacy* as being able to decide freely to).[1] Thus, privacy allows for inner and outer freedom of an individual, helps building and assuring the personal integrity and autonomy, helps protecting his reputation, is enabling different forms of social self-representation in different social contexts.

All in all, privacy is considered as important since it is a *bequest value* and an *option value* at the same time (whereas the distinction between bequest values and options values goes back to Hubig 1993).[2] From the point of view of action theory, bequest values allow for the building/constitution of an acting agent whereas option values already rely on a constituted acting agent keeping him free from outer restriction so as to preserve his possibility of acting (by enabling him to decide freely and keeping him free from constraints/inherent necessities). Privacy is both, a bequest value and an option value. As bequest value, privacy first and foremost allows for the constitution of an acting agent by assuring personal freedom and autonomy, guaranteeing freedom from governmental interventions, or other societal institutions, parties or persons and thus allowing a person to build his own individual scheme of life (beginning already in the childhood). It is privacy that establishes a sphere of non-intervention which is crucial for self-fulfillment and the development of a personal identity. However, privacy is also an option value: Privacy is essential for regulating personal relationships and establishing different social roles in society, thereby providing us backstages/leeways for deciding and/or acting.

PRIVACY ISSUES WITH GOOGLE STREET VIEW

According to the directive 2007/2/EC of the European Parliament and Council, geospatial data is “any data with a direct or indirect reference to a specific location or geographical area” thereby often describing a spatial object which is further defined as an “abstract representation of a real-world phenomenon related to a specific location or geographical area” (Article 3 of the Directive 2007/2/EC of the European Parliament and of the Council). *Geospatial data* is therefore only *object-related data* and not initially subject to data protection laws (Forgó et al. 2008). *However – under certain circumstances – geospatial data could become personal data* (Resolution of the German top data protection authority “Düsseldorfer Kreis” on the provision of digital street views in the internet 2008; Forgó et al. 2008). This is the case, if 1) photos or photo-realistic views/models of spatial objects (i.e. a building or an estate) could be easily located by geo-coordinates and thus easily matched to its owner or residents and/or if 2) the data is – to put it more generally – able to describe personal affairs or matters (Resolution of the German top data protection authority “Düsseldorfer Kreis” on the provision of digital street views in the internet 2008; Forgó et al. 2008). In these cases, geospatial data is also subject to data protection laws. Then, the collection, storage, processing and dissemination of the data is only allowed, if the interests of the individuals, which are subject of the data, are not harmed and/or are not superseded by other rights and interests (such as homeland security) (Resolution of the German top data protection authority “Düsseldorfer Kreis” on the provision of digital street views in the internet 2008).

Picking up the above mentioned dimensions of privacy, privacy intrusions in the realm of geospatial data are of cognitive nature only and therefore mainly *intrusions on informational privacy* (with possible effects on decisional and local privacy in the future):

[1] By taking up the distinction between “freedom from” (negative freedom) and “freedom to” (positive freedom) one could easily reconcile the two apparently competing concepts of a ‘control theory of privacy’ and a ‘restricted access theory of privacy’. (For an in-depth account of both competing concepts, see Tavani 2008, p. 141 et seq.)

[2] By putting forward the distinction between bequest values and option values, we propose yet another way – in our eyes fruitful way – of elaborating on the questions on ‘what kind of value privacy is’ and ‘why privacy is valued’ (for an overview on these existing discussions, see Tavani 2008, p. 156 et seq.).

1) Geospatial data showing faces of people, license plates of cars (as Google Street View does) could be regarded as problematic, since it conveys a lot of information on personal affairs, such as personal habits, preferences, circumstances of living (Resolution of the German top data protection authority “Düsseldorfer Kreis” on the provision of digital street views in the internet 2008; Privacy International 2009).

2) The same is true for showing house numbers and detailed, photo-realistic images or representation of spatial objects, since it tells a lot about personal circumstances and thus could allow for geo-marketing or scoring of creditworthiness (Resolution of the German top data protection authority “Düsseldorfer Kreis” on the provision of digital street views in the internet 2008; Privacy International 2009).

3) Especially Google Street View is criticized for having a “privileged view” on the spatial object: Pictures are taken at the height of 2.5m and not at the height of the eyes of a pedestrian, thus allowing to look inside an estate or home – a per se secured, protected, intimate space (Privacy International 2009).

However, data protection officials also agree on this: If the spatial object is obfuscated or the presentation of the spatial object is of abstract manner only, no interests of individuals are violated (Resolution of the German top data protection authority “Düsseldorfer Kreis” on the provision of digital street views in the internet 2008). Thus, privacy seems to be easily preservable by using different abstraction and obfuscation techniques.

POSSIBILITIES AND LIMITATIONS OF PRIVACY-PRESERVING ABSTRACTION AND OBFUSCATION TECHNIQUES

The commonly used approach to preserve privacy in Google Street View is the pixelating-out approach. Faces of people and license plates of cars are automatically pixeled-out / blackend by some image recognition software before providing the images in the internet (Spiegel Online International 2009). However, this solution has some major drawbacks. 1) The method is reported to work not reliably still leaving some faces and license plates unobfuscated (Privacy International 2009). 2) Even obfuscating parts of a person/object is not enough. In most cases, a lot of other distinctive, individual characteristics remain unobscured, still allowing for the identification e.g. of a person by the clothing he wears, the shape of his body, the height, his posture. These distinct characteristics (of spatial objects and/or persons) could be very small or unusual, which makes it nearly impossible to automatically detect and remove them all by automatic image processing. Even if it would be possible, the resulting images would depict scenes where large parts are blurred or missing. As such images are not attractive to anyone, this is obviously not a viable solution.

Another more radical approach (taken e.g. in Germany) is to grant the people affected by the photo taking the right to get the whole images removed from the database (Spiegel Online International 2009). But also this solution has its pros and cons. On the one hand, completely removing an image is definitely a very secure method. On the other hand, this assumes, that the person has been informed about the image capturing (before or afterwards) and that he can easily file objections against their publication. Second, the same holds true as for the first method. A lot of missing images/parts of a street view could render the service in a whole unusable or at least very unattractive.

The only viable alternative seems to be therefore to use image sequences that show the same scene at different times and/or from different angles. Then the critical objects are hopefully gone or at least are located in a different part of the image and have cleared the view to the formerly occluded area. Multiple images allow for an *image fusion* to produce new ones without people and private objects. Most comparable work has been done for this in the realm of the automatic *generation of façade textures (for 3D city models)* from terrestrial images, where occlusions from cars and pedestrians are avoided by a filtering of multiple images. Böhm 2004 e.g. blends per-pixel registered images in a color clustering approach in order to synthesize occlusion-free texture images for building façades (see Figure 1). By capturing a handful of images from multiple stations (or a sequence of images from one point), both moving and static objects that are in front of the façade can be completely eliminated.

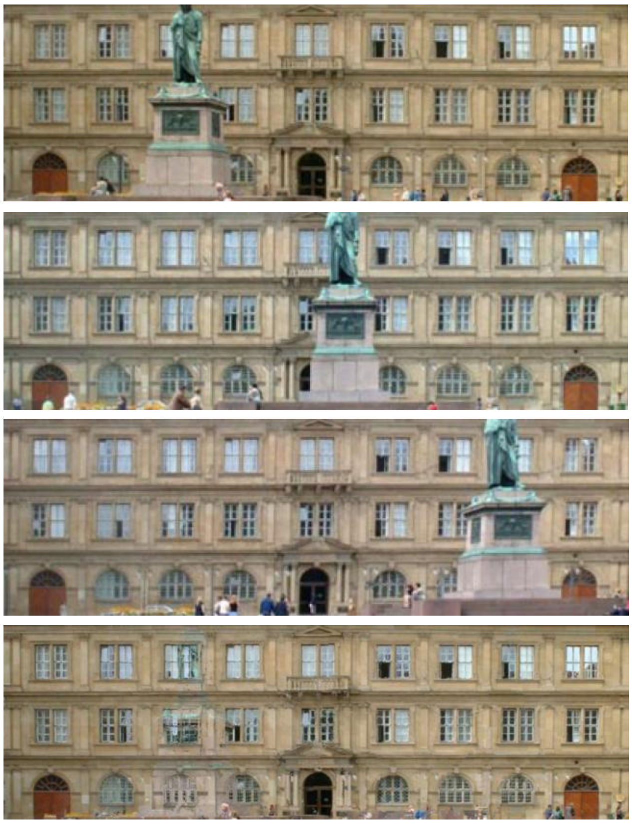

Figure 1: Occlusion-free texture (bottom) by multiple image fusion (Böhm 2004)

However, each pixel must exactly point to the same planar part of the façade as the corresponding pixels of the other images. Such image correspondences can be reliably determined by the SIFT operator (Lowe 2004), which has also been implemented to run in real-time (Sinha et al. 2006). Although an automatic retouching of façade images is only possible if the underlying façade geometry is known, the necessary methods for a reconstruction from stereo imagery and laser scanning data at street level has long been shown (see e.g. Früh and Zakhor 2004; Cornelis et al. 2006; Pollefeys et al. 2008). And as recent reports have stated, the Google Street View vehicles of Google have been spotted with laser scanners mounted on the roof (Shankland 2008). Now it also becomes clear why we have claimed, that the images of Google Street View are data of an interstage product only, data that – because of all the privacy issues – should have never reached the public. Google Street View data is data which serves just as an input for the construction of "sound" 3D city models where a lot of privacy issues have been removed by image fusion for the automatic occlusion-free generation of façade images.

However, within 3D city models, there are even more methods available so as to preserve privacy. Until now, we have only regarded objects that are *in front of the façade* and *not on the façade*. But the nature of the façade itself and objects on the façade (such as house numbers, name plates and billboards) are also of interest when trying to preserve privacy. Although stores, firms and companies place name plates and billboards by the majority for advertising purposes, private persons and small firms might feel their privacy violated by this unwanted publicity. Such objects and housing numbers could be detectable by optical character recognition (OCR), which has reached a level where letters and numbers are reliably recognized. The question remains what to do with these areas? In contrast to persons and cars, a blurring of the characters would in most cases be sufficient to make them unrecognizable. Again, such an approach is not very appealing as it degrades the quality of the façade textures. Better would be to retouch these areas by copying similar parts of the façade image (see Figure 2 bottom).

Once the objects in front of the building have been eliminated and the façades been cleared, the next level of anonymization is to remove what can be seen of the interior of the building. The major intrusion into private homes can be expected coming from the windows. To counteract this, the glass parts could be grayed out and given a bright streak of reflected light to keep a realistic appearance. Another option would be to store the semantic information, so that a visualization application can adapt the window glass to better reflect the environment and weather conditions (see Figure 3). However, before the relevant pixels can be altered, the locations and shapes of the windows must be detected. Several publications have addressed this problem. By using the Förstner operator (Förstner and Gülch 1987), Reznik and Mayer match façade images to a database

Figure 2: Two abstraction levels (1st image, 2nd geometry) from a photo-realistic 3D building model (top).

Figure 3: Hidden window contents (left) in comparison to original situation (right)

containing images of common window types (Reznik and Mayer 2007). This enables the identification of the position and dimensions of the windows. Ripperda and Brenner reconstruct the arrangement of doors and windows in a stochastic Reversible jump Markov Chain Monte Carlo process using formal grammars of façades (Ripperda and Brenner 2009). Becker and Haala detect 3D edges in image pairs to do a hypothesis test on the existence of glazing bars and fanlights of windows and doors (Becker and Haala 2007). Also Wenzel et al. detects repetitive structures in facade images by using the SIFT operator in conjunction with a heuristic search method (Wenzel et al. 2008).

However, a photorealistic visualization might not always be necessary in all applications. Döllner and Kyprianidis e.g. present an automatic image abstraction approach that, applied to image sequences of 3D city models, results in a realistic, but cartoon-like presentation of virtual environments (see Figure 2 center, Döllner and Kyprianidis 2009). On the one hand, such a presentation of real-life objects features enough details to recognize the spatial situation, but on the other hand changes enough to make re-identification of persons impossible and the judgment on people's living conditions inconclusive.

In a last image abstraction step, the facades and roofs could either be textured using generic textures or colored in a single color only (derived as mean color of the texture).

The abstraction of (façade) images is only one aspect concerning the privacy of geospatial data. Another is the *abstraction geometry,* which can be regarded both by single buildings, but also by their arrangement into building blocks. Concerning the alteration in terms of geometry, the following approaches may be used to ensure for obfuscated details:

1) Simplification of single buildings for cartographic purposes (e.g. Forberg 2004; Thiemann and Sester 2004; Poupeau and Ruas 2007; Kada 2005): Geometric simplification of models which are less important to the application's context to avoid revealing private information about someone's living conditions (e.g. the removed dormer in Figure 2 bottom).

2) Façade typification (Thiemann and Sester 2004): Change of the number and arrangement of façade elements in order to obfuscate the appearance of highly detailed façade models while maintaining the overall appearance.

3) 3D building symbols, standard roof shapes (see e.g. Thiemann and Sester 2006; Kada 2007): Replacement of the building roof shape or even complete building model by similar models from a standard library.

4) Typification (Sester 2000): Replacement of a group of models similar in shape and appearance by a smaller, re-located group, thus obfuscating the spatial situation or even hiding buildings that are at risk concerning their security.

5) Aggregation of building blocks (Anders 2005; Glander and Döllner 2008): Replacement of individual models by a single building block model, herewith hiding borders of single buildings from the user, while maintaining landmarks, if needed.

The possibility to use various combinations of these methods for geometric abstraction together with the aforementioned façade image approaches leads to a wide range of differently strong privacy-enhancing obfuscation techniques for 3D building models, which may be derived from the data delivered by StreetView and similar systems.

CONCLUSION

In this paper, we gave – from a philosophical and engineering point of view – an in-depth discussion on privacy in general and privacy issues within geospatial information systems in special. Claiming, that Google Street View is an interstage product only, which should have never reached the public, is maybe put a little bit too blatant. However, when discussing the different "adjusting levers" for privacy in 3D city models, it became clear, that all the privacy issues known from Street View are gone there and that indeed Street View data serves as a mere input for the construction of 3D city models, namely for the automatic generation of photo-realistic, occlusion-free façade textures.

Although there are many ways to preserve privacy within 3D city models, one has to bear in mind, that the core of data protection is not met by that. Especially in Germany, the data protection officials want to force Google not just to obfuscate Street View images and grant individuals the right to get certain pictures removed from the database, but also force Google to delete all non-obfuscated raw-data (so as not to be able to use the data anymore for e.g. commercial purposes in countries where data protection laws are not as strict as in Europe). And indeed this is the case: Google has collected data in Germany but has transferred all data for storing and further processing to the US thereby not willing to delete the raw material and therefore the data still being open for abuse and possible privacy violations.

But also with more or less photorealistic 3D city models, the question remains the same: Does our society want this technology or is it too big a threat upon privacy? Thus, all in all, it should be highly appreciated, that privacy and geospatial data is discussed more and more on a broad scientific as well as on a broad public basis. However it is not the job of science to rule on this matter. Its job just is to accompany, support and guide these debates, to clarify things and to outline and provide different solutions. The given paper is to be understood as such a contribution.

ACKNOWLEDGMENTS

This interdisciplinary work has been developed within the Nexus project (collaborative research centre/SFB 627 "spatial models for context-aware applications"), which is funded by the German Research Foundation (DFG).

REFERENCES

Anders, K.-H.: 2005, ‘Level of detail generation of 3D building groups by aggregation and typification’. In Proceedings of the 22th International Cartographic Conference, La Coruna, Spain.

Becker, S. and Haala, N.: 2007, ‘Refinement of building facades by integrated processing of LIDAR and image data’. In Proceedings of Photogrammetric Image Analysis PIA07, Munich, Germany, 7–12.

Böhm, J.: 2004, ‘Multi-image fusion for occlusion-free façade texturing’. In The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, Vol. XXXV, Part B, Istanbul, Turkey.

Cornelis, N., Cornelis, K., and Van Gool, L.: 2006, ‘Fast compact city modeling for navigation pre-visualization’. In Proceedings of the 2006 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, Vol. 2, 1339–1344.

Directive 2007/2/EC of the European Parliament and of the Council of 14 March 2007 establishing an Infrastructure for Spatial Information in the European Community “INSPIRE”. 2007. URL= http://www.emwis.net/documents/fol962872/euro_legislation/stl078838.

Döllner, J. and Kyprianidis, J.E.: 2009, ‘Approaches to image abstraction for photorealistic depictions of virtual 3D models’. In Proceedings of the First ICA Symposium for Central and Eastern Europe, 371–385.

Forberg, A.: 2004, ‘Generalization of 3D building data based on a scale-space approach’. In The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, Istanbul, Turkey, Vol. XXXV, Part B.

Forgó, N., Krügel, T., and Reiners, N. 2008. Expert’s report on geospatial data and data protection (German). URL=http://www.iri.uni-hannover.de/tl_files/pdf/Gutachten%20GEODAT.pdf.

Förstner, W. and Gülch, E.: 1987, ‘A fast operator for detection and precise location of distinct points, corners and centres of circular features’. In Proceedoings of the ISPRS Intercommission Conference on Fast Processing of Photogrammetric Data, Interlaken, Switzerland, 281–305.

Früh, C., and Zakhor, A.: 2004, ‘An automated method for large-scale, ground-based city model acquisition’. In International Journal of Computer Vision, Vol. 60, No. 1, 5–24.

Glander, T. and Döllner, J.: 2008, ‘Automated cell based generalization of virtual 3D city models with dynamic landmark highlighting’. In Proceedings of the 11th ICA Workshop on Generalization and Multiple Representation, Monpellier, France.

Hubig, C.: 1993, ‘Technikbewertung auf Basis einer Institutionenethik’ (German). In Lenk, H. and Ropohl, G. (eds.) ‘Technik und Ethik’; Reclam: Stuttgart, Germany, 282–307.

Kada, M.: 2007, ‘Scale-dependent simplification of 3D building models based on cell decomposition and primitive instancing’. In Spatial Information Theory: Proceedings of the 8th International Conference COSIT 2007, 222–237.

Kada, M.: 2005, ‘3D building generalisation’. In Proceedings of the 22th International Cartographic Conference, La Coruna, Spain.

Lowe, D.G.: 2004, ‘Distinctive image features from scale-invariant keypoints’. In International Journal of Computer Vision, Vol. 60, No. 2, 91–110.

Pollefeys, M., Nistér, D., Frahm, J.-M., Akbarzadeh, A., Mordohai, P., Clipp, B., Engels, C., Gallup, D., Kim, S.-J., Merell, P., Salmi, C., Sinha, S., Talton, B., Wang, L., Yang, Q., Stewénius, H., Yang, R., Welch, G., and Towles, H.: 2008, ‘Detailed real-time urban 3D reconstruction from video’. In International Journal of Computer Vision, Vol. 78, No. 2-3, 143–167.

Poupeau, B. and Ruas, A.: 2007, ‘A crystallographics approach to simplify 3D building’. In Proceedings of the 23rd XXIII International Cartographic Conference, Moscow, Russia.

Privacy International: 2009, ‘PI files complaint about Google Street View’. URL= http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-564039.

Resolution of the German top data protection authority “Düsseldorfer Kreis” on the provision of digital street views in the internet (German). 2008. URL=http://www.bfdi.bund.de/cln_118/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/141108DigitaleStrassenansichten.html?nn=409242.

Reznik, S. and Mayer, H.: 2007, ‘Implicit shape models, model selection and plane sweeping for 3D façade interpretation’. In the International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, Vol. XXXVI, 3/W49A, 173–178.

Ripperda, N. and Brenner, C.: 2009, ‘Application of a formal grammar to façade reconstruction in semiautomatic and automatic environments’. In Proceedings of the 12th AGILE Conference on GIScience, Hanover, Germany.

Rössler, B. The value of privacy; Polity Press: Cambridge, UK, 2004.

Rössler, B.: 2006, ‘New ways of thinking about privacy’. In Phillips, A., Honig, B., and Dryzek, J. (eds.) ‘The Oxford handbook of political theory’; Oxford University Press: Oxford, UK, 694–712.

Schoeman, F. Philosophical dimensions of privacy; Cambridge University Press: Cambridge, UK, 1984.

Sester, M.: 2000, ‘Maßstabsabhängige Darstellung in digitalen räumlichen Datenbeständen’ (German) (Postdoctoral thesis). Deutsche Geodätische Komission, Reihe C, Heft 544.

Shankland, S.: 2008, ‘Google Street View cars collect 3D data’. URL=http://www.cnet.com.au/google-street-view-cars-collect-3d-data-339289047.htm.

Sinha, S.N., Frahm, J.-M., Pollefeys, M., and Genc, Y.: 2006, ‘GPU-based video feature tracking and matching’. In Proceedings of EDGE 2006, Workshop on Edge Computing using New Commodity Architectures, Chapel Hill, USA.

Spiegel Online International: 2009, ‘Google bows to German data privacy demands’. URL=http://www.spiegel.de/international/germany/0,1518,631149,00.html.

Spiegel Online International: 2008, ‘Privacy concerns: German towns saying ‘Nein’ to Google Street View’. URL=http://www.spiegel.de/international/germany/0,1518,581177,00.html.

Tavani, H.T.: 2008 ‘Informational privacy: concepts, theories, and controversies. In Himma, K.E. and Tavani, H.T. (eds.) ‘The handbook of information and computer ethics’; John Wiley & Sons, Inc.: Hoboken, New Jersey, USA, 131–164.

Thiemann, F. and Sester, M.: 2006, ‘3D-symbolization using adaptive templates’. In Proceedings of the GICON 2006, Vienna.

Thiemann, F. and Sester, M.: 2004, ‘Segmentation of buildings for 3D-generalisation’. In Working Paper of the ICA Workshop on Generalisation and Multiple Representation, Leicester, UK.

Warren, S.D. and Brandeis, L.D.: 1890 ‘The right of privacy’. Harvard Law Review, Vol. 4, No. 5, 193–220.

Wenzel, S., Drauschke, M., and Förstner, W.: 2008, ‘Detection of repeated structures in facade images’. In Pattern Recognition and Image Analysis, Vol. 18, No. 3, 406–411.