Zentrum für Technologiefolgen-Abschätzung
Centre d'évaluation des choix technologiques
Centro per la valutazione delle scelte tecnologiche
Centre for Technology Assessment

Geographical signposts in cyberspace

Localisation technologies as a challenge for an open society

www.ta-swiss.ch

Informations about the study «Lokalisiert und identifiziert. Wie Ortungstechnologien unser Leben verändern»

The study was supported by the Swiss Federal Statistical Office FSO, by the Federal Roads Office FEDRO and by the Federal Office of Topography swisstopo

Lorenz Hilty, Britta Oertel, Michaela Wölk, Kurt Pärli

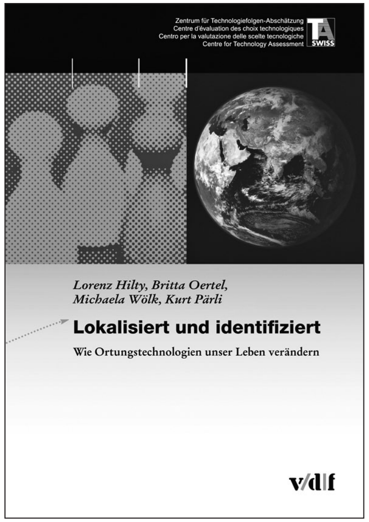
Lokalisiert und identifiziert
Wie Ortungstechnologien unser Leben verändern

TA-SWISS, Centre for Technolgoy Assessment (ed.).
vdf Hochschulverlag AG der ETH Zürich, Swiss Federal Institut of Technolgoy, 2012.

ISBN 978-3-7281-3460-8

Also available in open access:
www.vdf.ethz.ch/info/showDetails.asp?isbnNr=3460

Summary available online at www.ta-swiss.ch


Zentrum für Technologiefolgen-Abschätzung
Centre d'évaluation des choix technologiques
Centro per la valutazione delle scelte tecnologiche
Centre for Technology Assessment
TA SWISS
Lorenz Hilty, Britta Oertel,
Michaela Wölk, Kurt Pärli
Lokalisiert und identifiziert
Wie Ortungstechnologien unser Leben verändern
v/d/f

Contents

Localisation in brief

To be networked with the whole world, one no longer has to be sitting at a computer or by the telephone: with a laptop and mobile phone we can log on to the internet from virtually any location and hold telephone conversations anywhere. But when we do so, we leave traces which can be used to reconstruct our routes: mobile communication providers know when we have logged into a mobile phone antenna, and which one; internet service providers know our IP address, which enables them to work out our approximate position. When we use short-range radio technology (WLAN) to surf the internet, localisation is in fact relatively precise. In addition, more and more items we use every day are equipped with localisation functions.

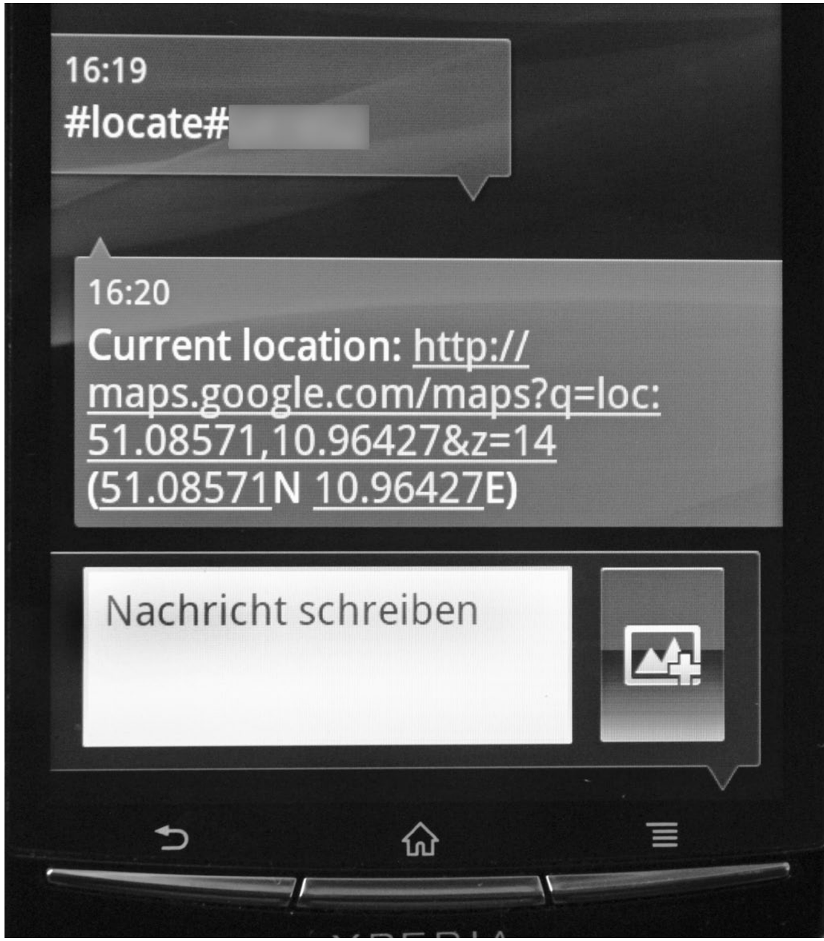
Localisation data are therefore increasingly becoming a basis for innovative business models and services. Localisation data in real time can, for instance, help the rescue services to locate victims of road accidents quickly. Stored movement profiles are also useful in traffic planning for identifying and clearing bottlenecks on the roads. However, there are also risks involved in handling location data. Someone who divulges location-related information too openly gives others an insight into their everyday life and habits. Social networks such as Facebook also tend to pass a great deal of personal information on to third parties which are interested in localisation data for marketing purposes with the result that these data are distributed across obscure pathways without the people concerned being aware of it.

The study «Lokalisiert und identizifiert. Wie Ortungstechnologien unser Leben verändern» by TA-SWISS aims to make people aware of the problem and put forward recommendations for handling location-related data.

Recommendations from the TA-SWISS study

Political and administrative decision makers are faced with a challenge in several respects:

- They must support measures enabling data protection to be implemented on an international level.
- To the extent that the organisation of rescue services, transport systems and other public sector areas is being based on localisation systems, these must be included in the Swiss programme on Critical Infrastructure Protection.
- It is also important for reliable and transparent software products to be certified so that data protection is made a quality characteristic of the relevant products.
- Furthermore, it is important to codify by law a limited storage period for localisation data; the people concerned should be given a kind of «digital eraser» so that they can enforce the right to forget with regard to their personal localisation data.
- Additional empirical research in the area of social sciences is needed to close knowledge gaps for dealing with localisation data.
- Finally, digital media competence must be generally improved, especially among young people to sensitise them to the opportunities and risks of putting their movement profiles and whereabouts online.



16:19
#locate#[redacted]

16:20
Current location: http://maps.google.com/maps?q=loc:51.08571,10.96427&z=14 (51.08571N 10.96427E)

The present abstract is based on the study «Lokalisiert und identifiziert. Wie Ortungstechnologien unser Leben verändern» (Localised and Identified. How Localisation Technologies Are Changing Our Lives), written by an interdisciplinary team headed by Lorenz Hilty, EMPA (www.ta-swiss.ch).

1 Geodata in transition between cyberspace and reality

An alibi often decides whether a person is convicted or acquitted. No coincidence there: loosely translated the word means «somewhere else», and stands for «not at the scene». In fact, information about where someone is, allows conclusions to be drawn as to what he or she does, sees and knows. Access to data providing information about who is in a precisely defined place at a specific time thereby opens up countless possibilities – both good and bad.

«Wow, c'est où ça?», posted a viewer of the digital photo collection of Jean-Frédéric Beaudet on March 15, 2010. The atmospheric snapshot shows a deserted warehouse where time seems to weigh heavily. It is only due to the warm light that the view over the dust-covered shelves and rusted steel girders evokes a sense more of nostalgia than unease. Visitors to Google's photographic portal Picasa could certainly have spared themselves questions about the location, because the coordinates of the subject appear on the right-hand edge of the screen: latitude 46.755165 degrees north and longitude 71.290497 degrees west. Google Maps gives this as the position of an abandoned industrial area on the outskirts of Saint Louis, a district of the Canadian city of Quebec. Thanks to Google Street View the abandoned hall can even be viewed from outside; the white graffiti-covered building looks a lot less artistic than one would have assumed from the inside view.

The photographic information also reveals that a Canon EOS Digital Rebel XTi was used – a model that is equipped with GPS receivers (Global Localisation System) and is able to automatically record data about where the picture was taken. More and more digital cameras and camcorders are fitted with GPS receivers. But even with an older camera, there is no need for anyone not to have so-called geotags thanks to a separate GPS tracker which can be linked to the camera by an external connection. And anyone taking a photograph or filming with a newer generation smartphone will also have the data for the place where the recording was made supplied by default with their pictures; if this application is deactivated on a mobile phone, other apps often no longer function.

Classification and espionage made equally simple

Many users of photography portals such as Picasa, Flickr, Fotocommunity or Locr value the supplementary localisation data because they allow them to find the location where the pictures published online were taken. The photography portal Panoramio even uses geographic data as a classification system for its collection. However, something that is not a problem with pictures of landscapes and urban impressions can, in the case of snapshots of private birthdays or wedding parties, lay a clear trail enabling nosy persons to pry into the lives of the people in the picture.

This can be well demonstrated using the online activities of a young family. Salomé and Klemens Christen-Kaiser were married in the early autumn of 2006; the picture uploaded onto a photography platform shows them on the day of their civil marriage ceremony with their daughter Gianna in front of the residential register office in the capital of the canton where they live. With her dark eyes and shock of brown hair, the little girl looks just like her mother – there are no signs of her father's mane of blonde curls. It also appears from the photo that Gianna was born eight months before the wedding: pictures show her as a baby in her pale yellow cardigan.

The cyberstalker's snooping trail

The collection of photographs published on the internet gives away a lot about the Christen family. It was put together by Patrick Siegenthaler, godfather to Gianna and long-time friend of Klemens. A school picture from the early 1990s shows the two as middle-school best buddies. If now, about 15 years later, the confectioner leaves the usual white icing off the young couple's wedding cake, that can be seen as a mere anecdote; far more revealing of his private sphere is the fact that Klemens is an outstanding sportsman. He looks really striking snowboarding in Saas Fee, and on various hikes. In the Swiss National Park for example he is one of the party («taken in Tarasp, Canton Graubünden, Switzerland», says the photo caption), and likewise on a cycling tour to western France («taken in Grayan-et-l'Hôpital, Aquitaine, France»). It is also significant that Salomé and Klemens have chosen a so-called wishing tree for Gianna in a large park in their town and regularly take photographs of their daughter there; anyone looking through the photographs in Patrick's collection for the corresponding location will find a series of pictures documenting her development from chubby-faced baby to little girl with a funny hairstyle.

Not once in publishing his photos does Patrick behave especially indiscreetly: the family names of Klemens and Salomé are not mentioned in any caption. It is the pictures of different sporting events in Patrick's collection – marathons, cycle and ski races – which ultimately give things away. Several photos show the couple as members of a team, and the event website includes the first and family names of all participants on the team pictures.

As a next step it is now easy to track down still more details about Klemens and his better half using social networks such as Facebook, LinkedIn or Xing: There it turns out that his wife is an evolutionary biologist who occasionally enjoys chopping wood in her spare time, while Klemens apparently works for an IT firm. The portraits on his employer's homepage confirm that it we are actually spying on the right person and not someone who happens to share the same name. The names of the persons described in this report have, by the way, been changed and some of the details of the locations shown in the photos have been voluntarily oversimplified. But the case is real and demonstrates that anyone who publishes personal data on the internet must bear in mind that some nosy character will uncover details about their lifestyle, personal relationships and habits. Without realising it, someone like Salomé who also regularly posts tweets on Twitter unwittingly provides further insights into their private life: their political sympathies and personal preferences are revealed – or the fact that they regularly use a certain rail connection.

Information about frequently used routes are in fact particularly informative, because human beings are creatures of habit. Studies show that if snoopers manage to analyse a person's movement profile over three months, that is enough to predict their whereabouts at any particular time with a 93 percent probability. Details about where someone likes to stay or lives are also very telling, because whether holiday photos were taken in Dubai or Engelberg, and whether one frequents youth hostels or five-star hotels, conclusions can be drawn about one's financial situation. And although the Christen family has deliberately chosen not to be listed in the telephone directory, with a little power of deduction their local community is quite easily tracked down. No need for an on-the-spot visit either: Thanks to services such as Google Earth or Street View, one then quickly determines whether their home is situated in a residential area, in a rural village or in a tower block.

Rue de la Jor
Ch. de la Batellerie
Prom. Robert Hainard
Rue de la Roselière
Rue du Parc
Rue des Mouettes
Le Petit Globe
Quai
Ch. des Bosquets
Prom. René-Be
Quai de Nogent
Parc des Rives du Lac
La Marive
Ch. du Sécheron
Av. de l'Hippodrome
Rue de l'Arsenal
Rue de l'Arsenal
Quai des Ateliers
Quai de l'Ancienne Douane
Rue de l'Ancien Stand
Yverdon-les-Bains
Av. de la Gare
Jardin Japon
des Remparts
Haldima
Rue de la Maison R
Rue du Lac
Rue du Milieu
Rue du Four
Rue du Pré

Different forms of localisation technology

- Satellite geolocation, Global Localisation System GPS: Originally developed for navigation in the military sector, the system based on geolocation by satellites is in use today in a very wide range of areas. In the open, GPS receivers can find their position with an accuracy of about 10 metres (apart from local coverage gaps caused by tunnels or buildings).
- Mobile phone localisation: In this case localisation is done using mobile phone antennae. The precision of the locational data also depends on the density of transmitter masts; under the most favourable conditions, in built-up areas, it is in the general order of 100 metres. The identification of individual mobile phones is done via the SIM card. Technically sophisticated mobile phones with internet access, so-called smartphones, are also fitted with a GPS module which enables more accurate localisation; in Switzerland most of the mobile phones that are sold are smartphones.
- Wireless Local Area Networks WLANs are used to wirelessly interconnect computers in close proximity to each other and to the internet. A WLAN base station enables wireless access to a local network. Mobile phone devices are positioned in relation to the base stations, provided these are listed in corresponding databases.
- Localisation via IP address: Every device needs an IP address to access the internet. Dynamic IP addresses are allocated by providers to the currently active terminals. Because each provider has a fixed number of addresses to allocate, with a known IP address the geographical location of the terminal can be reduced to a specific area. Precise localisation assumes that the provider discloses the connection data.

2 Localisation technologies for every purpose

The satellites for the Global Localisation System GPS were launched into orbit in the 1970s by the US military for the sole purpose of localisation and time measurement. The system is the best known, but certainly not the only tool for determining the location of human beings and devices. The widely used WLAN, as well as the internet addresses of computers and, of course, of smartphones also give away a person's location.

Klemens and Salomé often travel – as their photographs and blog entries reveal – by bike and by rail and tram. When they do, they could also make use of the timetables and travel information provided on their mobile phones by the transport companies – sometimes based with pinpoint accuracy on the location of the smartphone.

Mobility made easier

Even more extended excursions involving different means of transport and crossing tariff boundaries have become really easy for the Christen-Kaiser family thanks to localisation technologies: no more having to go to the ticket machine – all they need to take with them is the electronic ticket downloaded to their mobile phone in the form of a bar code. A project launched a few years ago in Switzerland under the name «ETIK», which is still in the development stage, is pushing the amenities even further. With ETIK, one no longer even needs to know the destination of an excursion in advance. A sensor installed in a small plastic card registers passengers contact free as soon as they get into a vehicle and then out again. Payment-relevant data, such as the point of departure and destination, time, type of car and the like, are captured, stored in the vehicle itself and transmitted to a server at close of business. It is a prerequisite for vehicles to be equipped with GPS in order to always determine exactly where they are. As well as advance payments using the prepaid method, billing at a later date would also be a possibility, and for the more distant future even a refinement of the tariff structure is not ruled out: hence flexible discounts could be granted if passengers travel at off-peak times, and there could also be a spontaneous and effortless change of class. In addition, extended offers such as the entry to a museum or the use of ski lifts could also be integrated into the electronic ticket. Incidentally, no actual movement profiles are created with ETIK: the data are anonymised and deleted after a set period of time.

As a keen winter sportsman, Klemens can also make use of developments in the field of avalanche localisation equipment. Those of the newer generation in addition to the normal radar are fitted with GPS receivers; this provides extra data for the rapid localisation of people who are buried, especially off-piste. In summer, the avalanche detection function can be switched off and the device used for off-road orienteering. It records the paths taken, which can then be downloaded onto the computer and shared with other bikers or hikers.

Their iPhones also allow Klemens and Salomé to benefit from the application that has been developed by the air rescue service Rega. In an emergency call, the app transmits also the locational data of the caller and thus speeds up the localisation process – gaining time that can save lives. The emergency call system eCall designed for road traffic by the EU is based on GPS and mobile telecommunication modules. The idea is that in case of an accident a control unit triggers an emergency call, and localisation systems switch themselves on at the same time. Thus no movement profiles are created, but the rescue service still receives the coordinates for rapid deployment. From 2015 onwards, new cars will be fitted with the new system; considerable advantages are expected in cases where accident victims are no longer able to communicate with the emergency switchboard, or for tourists not fluent in the local language.

It is not only geographical data concerning individual persons that are revealing. «Swarm monitoring» has advantages for traffic control in particular: if many mobile phones are only moving at walking pace on a motorway, there probably is a traffic jam. Such movement data are used not only to warn of traffic congestion, but can also be analysed for transport management, in order to structure road space according to the system needs.

Finally, localisation technology can help to optimise routes within a building. For instance, a new app for hospitals developed by the University of Bingen in Germany. When there is an emergency call it uses WLAN to send an alarm via mobile phone only to the doctors who are close by, thus saving time and avoiding a general rush.

Keeping in touch with friends thanks to social networks

More recently, localisation data have been a hot topic in connection with social networking. Many classic social networks such as Facebook, Google+ or Twitter are also offering a localisation function via their mobile apps. Newer communication platforms, like Foursquare or Yelp, have even been specifically designed for localised use. In this case, the user marks his own location on an interactive card and is able to see which of his «friends» are nearby. This is generally a matter of self-localisation; which means that users make their position known themselves by checking in at a specific «location».

With the messaging service Twitter for example, which restricts the length of the messages, the extra localisation function is a real plus – because one does not have to waste any of the allocated 140 characters at disposal on geographical data. The function is not enabled by default, but has to be activated by the users. With each entry, they can also decide whether or not they wish to disclose where they are. In spite of this comparatively exemplary handling of positional data, experts warn overenthusiastic «tweeters» of the dangers they incur. Anyone who frequently sends out status reports, and in doing so also discloses their positional data when they are out and about, indicates an empty home to potential burglars. Their creators may hail social networks as platforms for private exchanges between like-minded people; but they are hardly less interesting for the economy. The German service «friendticker», which can be used at no charge by private users, levies a recording fee for companies, and another charge for each successful check-in by a member. In the General Terms of Business, members also agree to receive advertising on their devices. Thanks to the localisation data, location-based micromarketing is now also becoming possible, with adverts being precisely tailored to the interests of the mobile phone owner. So one day Salomé could receive a message on her display about the vegetarian restaurant just round the corner, or about the nearest store for outdoor sports products.

Weighing up security against liberty

An IT expert like Klemens knows various ways of using localisation technology to prevent anyone stealing his laptop. There are a number of programs which can be installed on a device for this purpose. If the laptop goes missing, its owner logs onto a homepage, reports the loss and requests the positional data of the device. As soon as it is switched on, the laptop will transmit its location, which it determines using WLAN or – less accurately – via IP address. The media report cases where a theft victim shot a picture of the thief with the laptop camera and then published it on Facebook; the private hunt for the thief was reportedly crowned with success. There also exist apps for mobile phones which are able to locate a stolen or lost device.

To increase security in subways, railway concourses or on public transport, local authorities and companies are increasingly installing video cameras. Deploying them can actually help to enhance the feeling of security among passers-by. Many conductors on trams and buses also appreciate the cameras because they give them protection in case of incidents such as fights. Studies have now proven that video surveillance helps to prevent acts of violence and vandalism, especially on public transport. But here too geographical localisation data are created, because people are filmed in certain places – often without being aware of it.

Security is also top priority with systems for the surveillance of people. The electronic tags used to keep track of criminal offenders are well known. Police legislation in individual cantons, Basel-Landschaft for example, allows the use of electronic tags fitted with GPS if it is necessary to protect victims from violent partners or people stalking them. Thanks to the data that the system transmits, the authorities can control whether the person under surveillance is complying with the imposed exclusion order. A virtual protective fence is thus drawn around the person at risk that the stalker must not cross.

Paternalism or autonomy?

Digital security fences can also be designed in such a way that they prevent the person being protected from leaving a specific area. At schools in the US and UK, tracking systems have caused outrage. One school management was using localisation data not only to control the students' attendance in classes, but also allowing the provider to use the data to advertise its system. Many parents took offence at the data being reused in this uncontrolled and non-transparent way.

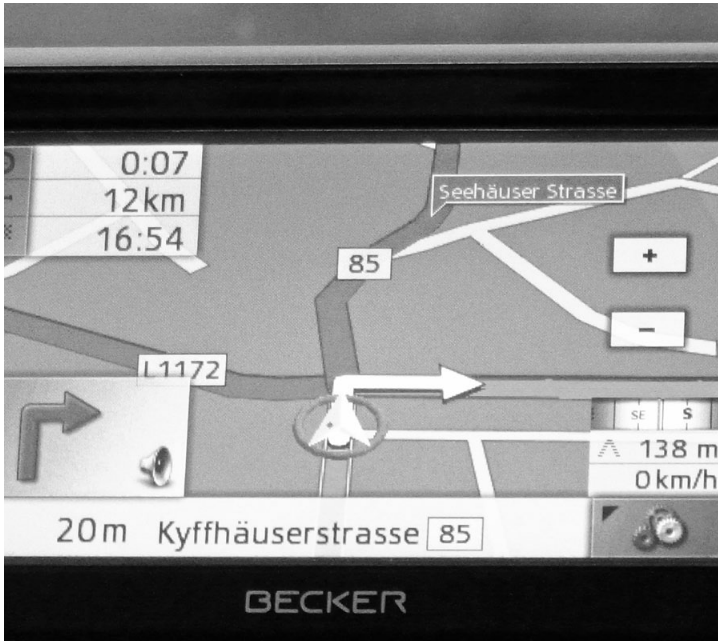
Finally, a virtual security fence can also be erected to trigger an alarm if persons at risk – Alzheimer's sufferers, for instance – leave a defined area. In this case, an armband with a localisation function can actually help to increase the freedom of movement for those affected, because otherwise they would have to be restrained by real fences in the hospital grounds. Nevertheless, when deciding whether to privilege the need for security or the striving for freedom, there is bound to be a conflict. In the case of people unable to articulate their interests themselves or to grasp the significance of decisions made on their behalf, it is especially important to carefully consider the balance between welfare and autonomy.

If government authorities have the means to spy on individuals – in the fight against criminality, for example – this is in the interests of society. In this case the police and public prosecutors are bound by clear legal regulations. However, the technology also gives private individuals the means of spying on third parties illegally. For example, the Thai software company Vervata has developed a small program that functions like a Trojan horse. It turns the mobile phone into a bug, and even sends telephone conversations or background noises – discussions during a meeting, for example – to the spies. Getting their hands on the smartphone for a couple of unguarded minutes is enough for them to install the «Flexispy» program. The software then transmits the data to a server in Thailand, which the snooper logs into and which is able to read the details of incoming and outgoing calls: telephone numbers, the names in the address book, the duration of the call and the like. Even the location of the mobile phone owner cannot escape the spyeye Trojan, which can also protocol the number of the transceiver base station that the mobile phone has just registered with. Flexispy was originally developed to catch unfaithful partners cheating on their spouses; today the German distributor recommends the program to «parents who would like to control their children's mobile phone», or wanting to locate their offspring «via GPS signal». Let us hope that the marriage of Salomé and Klemens lasts long and remains happy – or at least that they won't resort to illegal spyware from a shady underworld if they do separate.

Where am I – and where are my data?

In social networks, users give away a quantity of data that can find their way to third parties on far from transparent routes. As it says in the Facebook data protection guidelines: «We may also make information about the location of your computer or access device and your age available to applications and websites in order to help them implement appropriate security measures and control the distribution of age-appropriate content.» The user is not given precise information about exactly to whom and for what purpose Facebook passes on the data. It would, however, be naïve to assume that the prime concern of Facebook founder Mark Zuckerberg is user safety. It is quite clear that the collected data are of considerable value for the marketing activities of a very wide range of firms, willing to pay dearly to get their hands on the personal details and messages of internet surfers. The Gnip company, for example, specializes in collecting publicly accessible data on Facebook, Twitter and other platforms and selling them on for marketing purposes. Anyone wanting to read half of all tweeted messages, for example, has to pay 360 000 US dollars to do so.

But contrary to wealthy companies, private individuals have a much harder time obtaining information about all the data collected about themselves. The Austrian law student Max Schrems, for example, first had to file a complaint against the social network via the «Europe vs Facebook initiative» he launched after the network had refused to give him a copy of all of the information it had been keeping on him. The content of the CD-ROM which he eventually obtained amounted to 1222 printed pages including copies of posts he had deleted months earlier.



The cult iPhone has also been affected by a major scandal. In April 2011 it was discovered that iPhones and iPads working with the iOS4 operating system were gathering location data and storing them on a local file in the mobile phones' memory, so that the routes taken by their users could be reconstructed. In South Korea, a country whose inhabitants are very open-minded with regard to new communication technologies, 26 000 of those affected nevertheless brought actions against Apple.

3 Protect personal data

The technical resources for collecting and processing data are leading to more and more personal data being stored. It means that there is virtually no way of retaining control over our data – even if data protection laws give us the means to do so. But in the world wide web, national laws are extremely hard to implement and enforce.

As the online daily live of the Christen family demonstrates, the numerous databases and communications platforms on the internet enable private individuals with no hacking skills whatsoever to spy on the life and habits of other people. On the surface, such actions may even seem perfectly legal: after all, Article 16 of the Constitution of the Swiss Confederation, relating to freedom of opinion and information, states that everyone has the right «freely to receive data, to procure and to distribute date from generally accessible sources». The Swiss Data Protection Act also confirms, in its third section, that there is no infringement of privacy when personal data is processed by private individuals, «if the person concerned has made the data generally accessible and not expressly prohibited their processing». However, there is a general agreement among lawyers that social networks should not be regarded as generally accessible platforms, because many entries can only be read by other members of the network. Also, the networks themselves offer their users the facility to block strangers from seeing their pictures and postings.

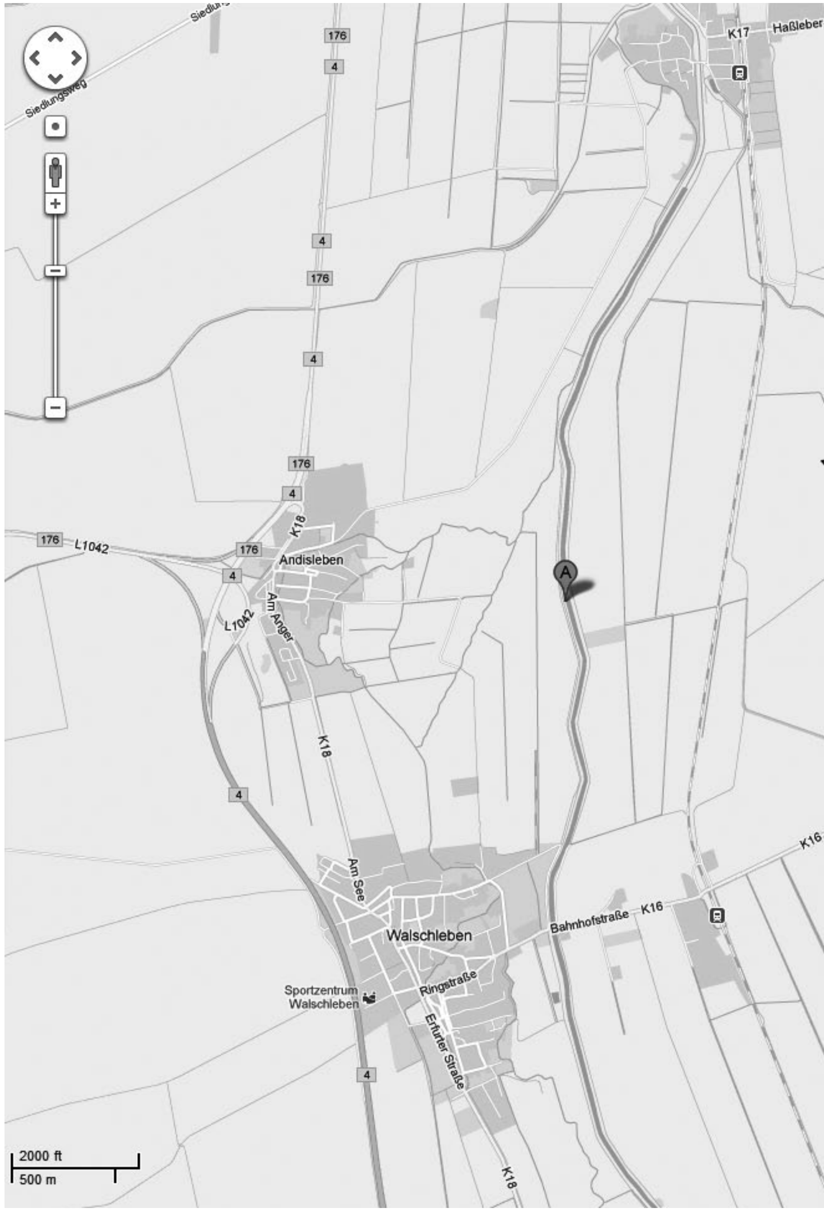
But in the case of geographical localisation data, is it actually about personal data anyway? Article 3 of the Data Protection Act suggests that the answer to this question is yes. It defines personal data as «data that relate to an identified or identifiable person». Information about routes followed on a regular basis can, in this sense, reveal the activities or the residence of a person and hence ultimately their identity. Geographical localisation data may potentially even be regarded as «sensitive personal data» – for instance if images that were taken close to a political event lead to speculation about the convictions of the person concerned.

Guaranteed loss of control

There is one major problem with the unlimited storage period for data published on the web: in reality, people who blog and publish photos over a number of years lose track of their data. Control over whether the data are pulled from their original context reappearing somewhere else on the internet later on increasingly eludes them.

Another thorny issue is that third parties can also publish information about and photos of people they know – as happened in the case of Salomé and Klemens in Patrick's photo collection. The couple themselves show much more restraint in their own blogs and photo uploads. The portraits both of them posted on social networking websites, for example, only show part of their faces: a tied-back strand of hair, a smiling eye, a cheeky piercing.

The problem is constantly being exacerbated by technical development: there are now face identification programs able to rapidly scan large amounts of photos and match single individuals. The social networks Google+ and Facebook have already integrated corresponding functions into their products. Automatic face recognition has recently made considerable progress, but still does not always function reliably. For the persons concerned, a wrong matching of images can cause just as big a problem as a perfectly correct profile that allows conclusions to be drawn about their lifestyle.



Abstinence is no solution either

Superficially, an individual can protect him or herself by refusing to publish personal data on information and communication platforms: someone who steers clear of social networks does not give any information away. However, digital abstinence also betrays a lot about a person, and can be interpreted to their detriment. Personnel managers who unsuccessfully search the popular social networks before a job interview for information about the candidates might assume that the person concerned has something to hide, or at least is a distrusting individual with limited team skills. Thus even missing trails on the internet can result in a person being discriminated against.

It has come to the point where more and more localisation data are being harvested in the public domain – for instance when surveillance cameras are installed to prevent criminal activities or vandalism. Only someone who steers clear of the corresponding sites can evade localisation of his or her whereabouts; ultimately, however, this means that the basic right of freedom of movement enshrined in the Swiss Constitution is curtailed.

Legally questionable misuse

As stated in Article 4 of the Swiss Data Protection Act, personal data must only be processed for the purpose «that was indicated at the time of purchase, and that is clear from the circumstances or provided for by law». If one takes this principle literally, most social networks are acting in a questionable way. Users provide their data to contact their «friends» and exchange news; the fact that the business principle of the platform is based on selling the data for marketing purposes is not immediately obvious to the layperson «from the circumstances».

Nevertheless, with detailed and standard terms and conditions that are not always easy to understand, Facebook & Co. justify the passing on of data by saying, for example, that minors should be protected and that information provided by third parties should be tailored to the interests of users. In fact, the social networks stipulate that users waive protection of their personal data. The data protection authorities are, to say the least, doubtful as to whether this informed consent is legally valid. And even if users disclose their location in connection with other applications, on their iPhone for example, in doing so they are not giving the receiver a free pass to reuse the data in any way.

General shortcomings in enforcement

In principle, the Swiss Data Protection Act gives people who consider that their right to privacy has been infringed a number of ways of defending themselves. Accordingly, the party making the complaint can demand that processing of data be stopped, that no further data be passed on, or that personal data be corrected or destroyed. However, appealing to national data protection legislation is hardly likely to impress internationally operating providers like Facebook or Google. Max Schrems was unable to get the social network to hand over his data until he launched a public initiative and gained the support of the Irish authority, which is responsible in this case for data protection in Europe, since Dublin is the home of Facebook's European headquarters (see box page 9). The threat to its reputation may well have been just as much of a reason for Facebook to back down as the legal arguments.

It is, however, often the very wish for discretion which makes those concerned reluctant to defend themselves against infringements of their privacy and to insist on the protection of their data. Among other things, a legal challenge results in data that the complainant would prefer to keep secret having to be made accessible to even wider circles than would have been the case without a legal dispute.

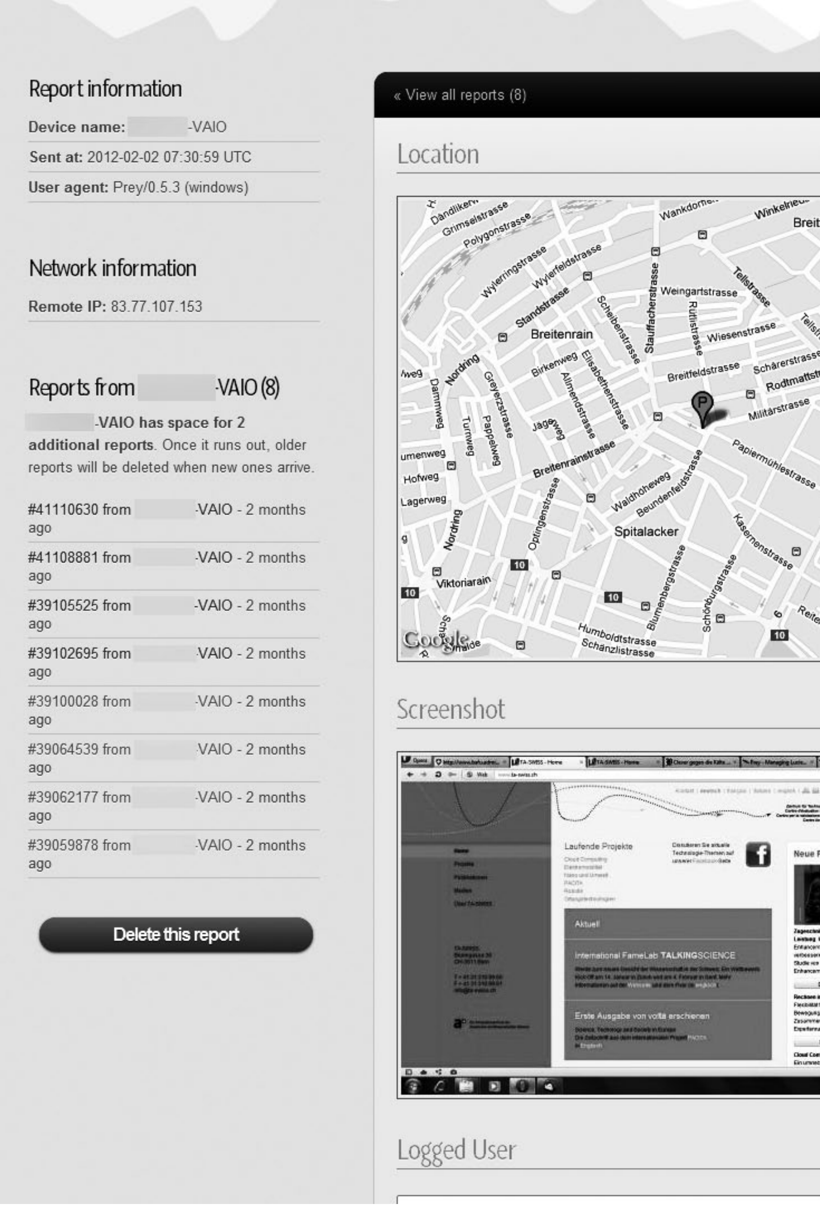
Global communication requires global protection

Many uncertainties about data protection legislation arise from the question of how far the coverage of the Swiss Data Protection Act actually extends if data is stored by a provider operating abroad. Jurists assume that the Swiss Data Protection and Information Commissioner (FDPIC) can intervene if data are processed in Switzerland itself. The question whether this precondition is met by social networks which operate from abroad is a contentious subject for lawyers, to say the least. In the case of international disputes, the question of responsibility must also be clarified.

Efforts to achieve stronger data protection are currently under way at a European level. The EU Commission is thus especially critical of references to data protection that are often unclear, difficult to find and non-transparent in online environments. The Commission also wants people to be given more control over the way their data are used. With regard to geolocation data, a consultative body of the EU Commission recommends that localisation services must be switched off by default, i.e. as part of the original factory setting. Furthermore, people who have agreed to the use of «their» localisation data should have to renew their consent annually, and be able to revoke it very easily. Providers would have to be obliged to switch on a permanent warning symbol for localisation functionalities which the user is unaware of.

Under the so-called Dublin and Schengen associations, Switzerland is obliged to enforce various EU legislative acts that are relevant to data protection laws. Modifications that the EU legislation has in mind with regard to the new technical possibilities would therefore be valid in Switzerland as well. This would mean that the data protection rights with respect to the processing of personal data of any individual would also be strengthened in Switzerland – a development that would certainly meet with approval from Salomé and Klemens. The reluctance and caution they exhibit in handling the privacy settings of their accounts, enabling only close friends to access their address and phone numbers, does in any case lead to the conclusion that they are very keen on protecting their personal data.

The internet thrives on the continuous, rapid updating of its content. The social networks are also constantly adapting their products, and in doing so often change the privacy templates that have to be filled in to determine who is given access to which data. Tips for privacy settings and a safer internet use can be found at:
www.datenschutz.ch
www.bsi-fuer-buerger.de
www.cnpd.public.lu (Commission Nationale pour la Protection des Données du Grand-Duché de Luxembourg)
www.europe-v-facebook.org/EN/en.html



Report information

Device name: [redacted]-VAIO

Sent at: 2012-02-02 07:30:59 UTC

User agent: Prey/0.5.3 (windows)

Network information

Remote IP: 83.77.107.153

Reports from [redacted]-VAIO (8)

[redacted]-VAIO **has space for 2 additional reports**. Once it runs out, older reports will be deleted when new ones arrive.

#41110630 from [redacted]-VAIO - 2 months ago

#41108881 from [redacted]-VAIO - 2 months ago

#39105525 from [redacted]-VAIO - 2 months ago

#39102695 from [redacted]-VAIO - 2 months ago

#39100028 from [redacted]-VAIO - 2 months ago

#39064539 from [redacted]-VAIO - 2 months ago

#39062177 from [redacted]-VAIO - 2 months ago

#39059878 from [redacted]-VAIO - 2 months ago

Location

Screenshot

Logged User

Study «Lokalisiert und identifiziert. Wie Ortungstechnologien unser Leben verändern»

Supervisory group

- Dr. Bruno Baeriswyl, Data Protection and Information Commissioner, Zurich; TA-SWISS Steering Committee (chairman of the supervisory group)
- Florence Bettschart, Consumers' association: Fédération Romande des Consommateurs FRC, Lausanne
- Alain Buogo, Federal Office of Topography swisstopo, Wabern
- Dr. Christine Giger, Giger GeoIT, Embrach
- Prof. Dr Gudela Grote, Work and Organizational Psychology, ETHZ, Zurich
- Dr. Jessica Heesen, Eberhart Karls University, Tübingen
- Rainer Humbel, Federal Statistical Office FSO, Neuchâtel
- Thomas Kallweit, FELA Management AG, Diessenhofen
- Dr. Francisco Klauser, Geography Institute, University of Neuchâtel, Neuchâtel
- Michael Kocheisen, Innovation Competence Center, Swisscom (Switzerland) AG, Bern
- Ulrich Lattmann, Swiss Academy of Engineering Sciences SATW, Zurich
- Urs Luthe, Federal Roads Office FEDRO, Bern
- Franziska Meister, Die Wochenzeitung, Zürich
- Cyrill Osterwalder, Google, Zürich
- Hans Kaspar Schiesser, Union of public transports, Bern
- Philipp Stüssi, The Federal Data Protection and Information Commissioner FDPIC, Bern
- Prof. Dr. Rolf H. Weber, Center for Information and Communication Law, University of Zurich, Zürich
- Dr. Franz Zeller, Federal Office of Communications OFCOM, Bienne

TA-SWISS Project Supervisors

- Dr. Sergio Bellucci, TA-SWISS
- Nadia Ben Zbir, TA-SWISS

Impressum

TA-SWISS (ed.). Geographical signposts in cyberspace. Localisation technologies as a challenge for an open society.

Abridged version of the TA-SWISS study «Lokalisiert und identifiziert. Wie Ortungstechnologien unser Leben verändern», Bern 2012.

TA 57A/2012

Author: Lucienne Rey, Bern
Editing: Christine D’Anna-Huber, TA-SWISS
Translation: Gary Williamson, Woking, Surrey (GB)
Layout: Hannes Saxer, Bern
Photography: Lucienne Rey
Printed by: Jordi AG – Das Medienhaus, CH-3123 Belp

TA-SWISS – The Centre for Technology Assessment

New technology often leads to decisive improvements in the quality of our lives. At the same time, however, it involves new types of risks whose consequences are not always predictable. The Centre for Technology Assessment TA-SWISS examines the potential advantages and risks of new technological developments in the fields of life sciences and medicine, information society, nanotechnologies as well as mobility, energy and climate. The studies carried out by the Centre are aimed at the decisionmaking bodies in politics and the economy, as well as at the general public. In addition, TA-SWISS promotes the exchange of information and opinions between specialists in science, economics and politics and the public at large through participatory processes, e.g. PubliForums and publifocus. Studies conducted and commissioned by the Centre are aimed at providing objective, independent, and broad-based information on the advantages and risks of new technologies. To this purpose the studies are conducted in collaboration with groups comprised of experts in the relevant fields. The professional expertise of the supervisory groups covers a broad range of aspects of the issue under study. TA-SWISS is a centre for excellence of the Swiss Academies of Arts and Sciences.

Centre for Technology Assessment
Brunngasse 36
CH-3011 Bern
info@ta-swiss.ch
www.ta-swiss.ch

A Centre for Excellence of the
Swiss Academies of Arts and Sciences

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Roads Office FEDRO

Federal Statistical Office FSO

Federal Office of Topography swisstopo