Law Enforcement 2.0 - The Potential And The (Legal) Restrictions Of Facebook Data For Police Tracing And Investigation

Sebastian Voigt  
*Technische Universität Darmstadt, Darmstadt, Germany*, voigt@emarkets.tu-darmstadt.de

Oliver Hinz  
*Technische Universität Darmstadt, Darmstadt, Germany*, hinz@wi.tu-darmstadt.de

Nora Jansen  
*Technische Universität Darmstadt, Darmstadt, Germany*, nora.jansen@web.de

Follow this and additional works at: [http://aisel.aisnet.org/ecis2013_cr](http://aisel.aisnet.org/ecis2013_cr)

**Recommended Citation**  
Voigt, Sebastian; Hinz, Oliver; and Jansen, Nora, "Law Enforcement 2.0 - The Potential And The (Legal) Restrictions Of Facebook Data For Police Tracing And Investigation" (2013). *ECIS 2013 Completed Research*. 5.  
[http://aisel.aisnet.org/ecis2013_cr/5](http://aisel.aisnet.org/ecis2013_cr/5)
LAW ENFORCEMENT 2.0 – THE POTENTIAL AND THE (LEGAL) RESTRICTIONS OF FACEBOOK DATA FOR POLICE TRACING AND INVESTIGATION

Voigt, Sebastian, Technische Universität Darmstadt, Hochschulstraße 1, 64289 Darmstadt, Germany, voigt@emarkets.tu-darmstadt.de

Jansen, Nora, Technische Universität Darmstadt, Hochschulstraße 1, 64289 Darmstadt, Germany, nora.jansen@web.de

Hinz, Oliver Technische Universität Darmstadt, Hochschulstraße 1, 64289 Darmstadt, Germany, hinz@emarkets.tu-darmstadt.de

Abstract

Innovative information technologies permit new approaches to fight crime. This study examines the police’s state-of-the-art application of Facebook information and identifies two fields of usage: First, the police use Facebook to ask users for help, e.g. looking for witnesses of a crime. Second, the police search the social network for information, pictures or social bonds of a specific person. As academic literature is amazingly quiet on this timely topic, this study compiles recent media reports and results from a German pilot project conducted by Hanover police. Although several success cases show the potential of this new approach, new areas of conflict, e.g. how to protect the privacy of prospective offenders or witnesses, are created in this way. Our analysis reveals that the regulatory framework for the police work on Facebook is unclear. Thus we provide policy makers with a list of legal issues that remain to be clarified. Additionally, we compile hypotheses that provide avenues for future research.

Keywords: Police, Facebook, Social Network, Tracing, Investigation, Legislation, Data Privacy.
1 Introduction

Since the 2001 terrorist attacks in New York, security concerns have increased worldwide. Not only intelligence agencies intensified the collection and analysis of information to investigate terrorists’ activities, but also local law enforcement agencies put more effort into modern information technologies (Chen et al., 2003; Custers 2012) which allow new approaches for public authorities to prevent crime and prosecute criminals, such as data mining (e.g. Abbasi and Chen, 2005), Policeware (e.g. Nabbali and Perry, 2004; Diffie and Landau, 2009), intelligent camera tracking (e.g. Lee et al., 2012), mobile phone and computer surveillance (e.g. Nettleton and Watts, 2006; COM, 2010).

Since a few years, police authorities use social networks such as Facebook for tracing and investigation purposes. In a simple case of an online tracing, the police may ask Facebook users for help, e.g. looking for eye witnesses of a crime or the whereabouts of a missing person. In Germany, we find 14 local police authorities who regularly post requests for information on Facebook and more examples in the UK and the US. Besides, the police use the social network to collect information about a person. With more than one billion monthly active users (Facebook, 2013a) sharing their pictures, social activities or interests, Facebook may be a useful source of information for the police.

Our work on the police’s state-of-the-art usage of Facebook data provides an overview on technological, societal and legal issues and the new areas of conflict created hereby. While the police may wish to use information gathered via Facebook most effectively, they must consider existing laws and regulations that protect the privacy of prospective offenders or witnesses. However, the existing regulatory framework may not always be as precise as needed. Our review has three main objectives: First, as it is (to our knowledge) the first scientific paper exploring police work on Facebook, we review how police authorities use Facebook today for tracing and investigation, and assess the potential of this new approach. Second, we study if the legislation in Germany provides a clear regulatory framework for the police work on Facebook. We identify legal “grey areas” and advise policy makers to focus on these existing legal issues. Third, we compile hypotheses that aim at stimulating researchers to conduct additional studies.

Interestingly, academic literature is rather quiet on this timely and important topic. To receive valuable information on the police’s usage of Facebook and its restrictions, we compiled dozens of recent TV, radio and newspaper reports from different countries. Additionally, we looked into the results from a pilot project conducted by Hanover police, approaches from other public authorities, contributions from the European Union and the German federal government, existing laws and judiciary decisions. We selectively spoke with police staff specialised in the field of Internet crime to verify our findings.

The remainder of this paper is structured as follows: we start examining how police authorities already exploit Facebook information. As we describe in chapter 2, Facebook allows the police to publish requests for information, to find suspects or witnesses and thus to gain important hints for an ongoing tracing. In chapter 3, we explore how Facebook information, e.g. taken from a suspect’s profile page, can be used to support an investigation. Both sections include a review on advantages and critical aspects of the authorities’ work with the network, as well as several success cases, partly taken from the Hanover pilot project. Chapter 4 dares an outlook on the police’s future application of Facebook. Chapter 5 concludes with advice for the policy makers and shows avenues for future research.

2 Police Tracings via Facebook

2.1 The process of tracings via Facebook based on a pilot project

Germany’s Polizeidienstvorschrift 384.1 (Official Police Instructions) defines a police tracing as the “[...] search for individuals or properties in the context of a criminal prosecution, sentence execution or danger prevention [...]”. The media used for tracings depend on the gravity of the crime and can include internal media such as police information systems as well as external media such as publishing
requests for information in newspapers, TV shows or on the Internet. In case the police use external media, we refer to public tracings. In such, the requested person must be under strong suspicion of having committed a serious criminal offence (Spiegel, 2012a; Bundestag, 2007). Section 131a (3) StPO (Strafprozessordnung; Code of Criminal Procedure) determines the structure of a public tracing. It also applies to tracings on the Internet and via Facebook.

In Germany, the police in Hanover are considered a pioneer for public tracings in social networks. They carried out a pilot project between February and August 2011, publishing identikit pictures on Facebook to trace accused persons (Deutschlandradio, 2012) and to support the investigation of a crime. If the police in Hanover decide to publish a request for information according to section 131a (3) StPO, a judicial decision has to be obtained first, according to section 131c (1) StPO. Only then a request for information, in many cases supported by an identikit picture with respect to section 131b StPO, is posted on the wall of the police’s (public) Facebook page (Süddeutsche Zeitung, 2011a). Facebook users can comment on tracing posts, however, the police always ask users to contact them via telephone. This way, the police want to avoid that personal details of accused persons or witnesses are published. Figure 1 shows the process of a tracing via Facebook and its legal basis in Germany.

Today, Hanover police are not the only police authority using Facebook for tracing purposes. In March 2013, we found 19 German police authorities who have a Facebook page, and 14 of them regularly publish tracings. Likewise, the FBI regularly post requests for information on Facebook. In the UK, Greater Manchester Police are a pioneer in Internet tracings by using Facebook and Twitter.

Figure 1. Tracing process via Facebook

2.2 Advantages of Facebook compared to common tracing tools

Large and active audience. The number of active users is a major reason why the police refer to the social network as a tracing tool. In December 2012, Facebook had more than a billion monthly active users worldwide (Facebook, 2013a) and about 25 million users in Germany (Statista, 2013). Thus, Facebook offers an enormous coverage that can be used by the police to reach more potential witnesses than via any other communication channel. While requests for information in daily newspapers are usually read more often by elder people, a social network can reach younger people more easily (Deutschlandradio, 2012). 27% of the Facebook users are between 18 and 24 years old (Statista, 2012), i.e. the most active age class of all Facebook users (Social Media Quickstarter, 2011). In March 2013, Hanover police’s Facebook page had more than 113,000 “Likes”, Greater Manchester Police’s had c. 41,000. Both Facebook and non-Facebook users can access the pages and support the tracing. Facebook users can share posts with their friends. Thereby, the police are able to reach a large number of people within a short time. The requests for information published by Hanover police between September 2012 and March 2013 have on average been shared 1,232 times by its users (Facebook, 2013b). Considering an average friend count of 190 (Facebook, 2011a), a request for information can quickly reach hundreds of thousands of users. Requests for information published on Facebook are not restricted to certain regions, but are available throughout the entire (global) network.
Fast medium. Compared to other channels, Facebook is a very fast communication medium. Requests for information can immediately be commented. Posting a request can provide crucial information helping the police investigation already within a few minutes. A newspaper, however, must first be printed and published, so requests for information are read at a later time.

No publication costs. Publishing requests for information on Facebook incurs no media costs. This allows the police to publish offences independent of their gravity. In this way, the police can also collect hints regarding tracings that might not have been published in newspapers or other costly media. Even though the users’ attention span for a post may be limited, the police are able to selectively repost the request for information at no cumulative costs. A tracing published on TV or in a newspaper incurs extra costs for every additional broadcast. So, it may only be perceived on its release date, and will not be available anymore for the remaining tracing period (NDR, 2011a).

2.3 Successful tracings via Facebook during the pilot project

During the pilot project in Hanover, 60 requests for information were published on Facebook to find criminals, witnesses and missing people (Hamburger Abendblatt, 2011; RTL, 2011). The posts were read about 150,000 times on average. Over six months, the police were able to solve eight cases with the help of Facebook users where previous tracings via other channels were unsuccessful (Spiegel, 2011a). In the following, we present some of these success cases (for details see Presseportal, 2011).

Theft. Hanover police were looking for three thieves. The investigations had been unsuccessful for four months. As a consequence, the police decided to publish pictures taken by a surveillance camera on Facebook. The offenders could be identified with the help of the network’s users on the same day (Süddeutsche Zeitung, 2011b). The case shows that Facebook is indeed a very fast medium. In another case, offenders stole a VW Polo in Wolfsburg and then committed a petrol theft near Hanover. The police in Wolfsburg asked their colleagues from Hanover for help. Common investigations were not successful, so the police decided to post a request for information on Facebook. A woman recognised the co-driver of the stolen car. With this information, the police were able to identify the driver.

Assault. A 17-year-old girl was attacked by two teenage girls. The accused girls were photographed by a surveillance camera. The police published the picture in regional newspapers (ARD, 2012), but received no hints to identify the offenders. A judicial order was issued allowing the police to publish the picture on Facebook. One hour after the post on the social network, the first useful pieces of information were given so that Hanover police could identify the two accused girls.

Missing children. In one case a 14-year-old boy had been missing for two days and in another case a 12-year-old girl had disappeared for three days. In both cases the police in Hanover asked Facebook users for help. The missing boy contacted the police via telephone himself 45 minutes after the publication went online. In the case of the girl, her friends saw the request and convinced her to return home. Both cases show that requests for information on Facebook can put a certain pressure on the missing persons or their social contacts (NDR, 2011a).

Rape. A 16-year-old girl accused two men of rape after a night club visit. She recognised one of the potential offenders in a picture taken by a surveillance camera. The picture and a request for information were published on Facebook in order to identify the prime suspect. A few hours later the man in the picture contacted the police in order to prove that he was not the person they were looking for. Besides he could even give them valuable information concerning the real offenders who later confirmed that they had sexual contact with the girl, but denied having raped her.

2.4 Critical aspects of Facebook tracings

Public rush to judgement. As seen in the previous case, Facebook tracings bear the risk that users publish hints that may not target the offenders, but (accidentally) charge innocents. As the next example shows, this can lead to a public rush to judgement. A 17-year-old teenager was suspected of murder. A neighbourhood girl saw the boy being arrested and spread the news directly on Facebook.
As a consequence, the young man was condemned in public (NDR, 2012a). By commenting posts, witnesses are able to publish the full name of a potential offender. Thus, in every request for information, the police ask witnesses to call them instead of commenting the post. The problem is that the comment function on Facebook cannot be switched off. Such comments can also contain wrong denunciations pillorying innocent people (ZDF, 2012; Spiegel, 2012a). Furthermore, giving hints by commenting on Facebook requests for information can also have consequences for the authors. Their names and comments are available for every Internet user. Thereby, users might even become a target.

**Insufficient data protection for witnesses and potential offenders in the social network is criticised.**

**Data storage/data deletion.** Protecting sensitive information related to public tracings may conflict with the fact that Internet data is usually stored forever: search engine operators make backups of websites on a regular basis, and any Internet user has the possibility to copy and save online content (Lawblog, 2012). Copies of requests for information and related comments could still be found on the Internet beyond the tracing period. This could have serious consequences for innocent people and for those who have been acquitted in a trial or have served their sentences (NDR, 2012b). Those people might be associated with certain crimes or suspicions forever and be disadvantaged thereby.

Another issue is that Facebook data generated by users – including the police – cannot be completely deleted by these users. The data is only marked as deleted and cannot be seen by users any longer, but it is still saved in Facebook’s databases (HR, 2012; Heise online, 2012a). Facebook states in its data policy that they “cannot ensure that information you share on Facebook will not become public [...]” (Facebook, 2013c). This makes the exploitation of Facebook data for police purposes rather critical.

**Legislation.** Until now there are no laws that control tracings via Facebook. They are justified with the interpretation of section 131a (3) StPO. Appendix 2, Section 3.2 RiStBV (Richtlinien für das Strafverfahren und das Bußgeldverfahren; Guidelines for criminal and summary proceedings) says that public tracings on the Internet should be conducted on police websites. Private websites should not be used. However, these are only guidelines for public authorities and no legal basis (Zeit, 2012a).

The storage of Facebook’s data on US servers is seen as a major problem (Hamburger Abendblatt, 2011). All data belonging to Hanover police’s Facebook page is stored in California. This includes profile data and IP addresses of users and visitors. Data protectionists criticise the transmission of personal data to the US since the police do not have any influence on what is happening to that data (ULD, 2011). Data protection specialists and police unions demand an update of the German data protection laws (Hamburger Abendblatt, 2011; Spiegel, 2011b). The first version of the German BDSG (Bundesdatenschutzgesetz; Federal Data Protection Act) came into force in 1979, long before private Internet and Facebook usage, the last amendment was made in 2009. Thilo Weichert, data protection commissioner in Lower Saxony, emphasises that tracings via Facebook are not compatible with German and European data protection laws (Spiegel, 2011b). He refers to the following situation: Facebook’s headquarters are in the US, but the central office in Dublin, Ireland, is in charge of data processing for European users (ULD, 2011). Thus, European or Irish law should be applied. But the social network’s conditions of use are based on American law which is less strict (ZDF, 2011).

According to European law, Facebook must inform its users how their data is used and analysed. As this is not the case, the social network violates Article 10 of the 95/46/EG directive (European Union, 1995) which states that “data-processing systems [...] must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy [...]”.

**Personnel expenditure.** When requests for information are published on Facebook, they must be supervised and maintained continuously. The police must follow all provided information, even if it does not seem useful (RTL, 2011). In case the police want to prevent users from publishing hints or personal information through Facebook’s comment function, they permanently need to supervise the site and delete objectionable posts (Heise online, 2011). On a platform like Facebook, a large number of comments can raise in a short time which can lead to increased personnel expenditure.

Table 1 summarises the main advantages and critical aspects of tracings via Facebook.
The police use Facebook not only to trace suspects and victims, but also to investigate actively in order to expose and prevent criminal acts. In this section, we present the advantages of the Facebook use in police investigations, show success cases, and close with (legal) limitations.

<table>
<thead>
<tr>
<th>Advantages</th>
<th>Critical aspects</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook tracings can reach a large (especially young) audience</td>
<td>Wrong denunciations on Facebook risk to create a public rush to judgement</td>
</tr>
<tr>
<td>Facebook tracings are not limited to certain regions</td>
<td>Facebook data cannot be completely deleted, which may penalise innocent or acquitted people</td>
</tr>
<tr>
<td>Medium is very fast, enables quick continuation of investigative work</td>
<td>No clear legal basis, interpretation of section 131a (3) StPO for tracings via Facebook is disputed</td>
</tr>
<tr>
<td>The police can (re)post a request for information without extra costs</td>
<td>Facebook does not apply European data protection laws</td>
</tr>
<tr>
<td>Requests for information can be published, independent of the offence’s gravity</td>
<td>Higher personnel expenditures may be required to supervise Facebook tracings</td>
</tr>
</tbody>
</table>

Table 1. Advantages and critical aspects of tracings via Facebook

Consequences for the continuation of tracings via Facebook. The pilot project in Hanover has been considered successful. The police continued to publish requests for information beyond the end of the pilot project in August 2011. From January to February 2012, tracings via Facebook were stopped because of legal concerns. The main reason was the transmission of personal data (i.e. detailed descriptions of suspects incl. identikit pictures, requests to post hints on Facebook) to servers in the US. In February 2012, tracings via Facebook were resumed after having changed the information policy. First, Hanover police ceased posting the detailed description of suspects and identikit pictures on Facebook. Instead, this information is only available on the police’s website which can be accessed through a link published on the social network. Other German police authorities, e.g. from Cologne or Erfurt, did not adopt the Hanover approach and still post suspect descriptions and identikit pictures along with requests for information. A consistent national information policy remains to be passed. Second, Hanover police ask all users to only provide information via telephone, not via the comment function on Facebook. These two measures minimize the amount of sensitive data transferred to the US. Figure 2 points out which information has been published during the Hannover pilot project in 2011 and what is published today on Facebook. It rests upon a request for information published in January 2013.
3.1 Advantages of using Facebook for police investigations

**Exposure of criminal acts.** The information in social networks is often very valuable for the police. This includes a person’s residence, occupation, friends, attitudes and hobbies (Spiegel, 2011b; Gross and Acquisti, 2005). Depending on the user’s privacy settings, this information can be available to anyone. If a user’s profile is public, the police can use the information without any restriction. If this is not the case, investigators may ask Facebook to hand out necessary information. Facebook is bound to give “US security agency an insight into their membership data” (Hamburger Abendblatt, 2011). American police authorities can access it if a “valid subpoena [...] in connection with an official criminal investigation”, “a court order [...] under 18 U.S.C. Section 2703(d)” or “a search warrant” have been issued (Facebook, 2013d). Non-US authorities need a letter rogatory to access the data.

Police staff can also work under false identity to access information, as six BKA (Bundeskriminalamt; Federal Criminal Police Office) investigators do. They send friend requests to suspects (Bundestag, 2011) and then examine the social life of a person. The police can act if abnormalities occur, identify whereabouts of suspects or get personal information of friends who might support the investigation.

Using specialised Facebook search software is another way to extract information. Europol, European Union's criminal intelligence agency, already uses social network analysis tools (Heise online, 2012b) that aim at identifying and analysing relations between persons. Breadth and depth of such information are usually more extensive than those available in police databases. Such “profile crawlers” can access a person’s private information through his social network. Kosinski et al. (2013) show that Facebook “Likes” can be used to accurately predict a range of sensitive personal attributes that might help a police investigation, including age, sexual orientation, ethnicity, religious and political views, personality traits, intelligence, happiness or use of addictive substances. The crawler may even abuse common Facebook weaknesses. E.g. even in case the searched person’s profile is only accessible by friends, the list of friends is usually accessible and serves as a starting point for the progressive search (Balduzzi et al., 2010). Likewise, it is even possible to make predictions regarding the acquaintance between two non-Facebook members with a high rate of success (Hovrát et al., 2012).

**Prevention of criminal acts.** In Canada and the US, police and FBI use Facebook to recognise criminal behaviour before a crime is committed. For example, authorities supervise prisoners’ Facebook use (San Francisco Chronicle, 2011) and scan public profiles from US high school students to prevent acts of violence at schools (Washington Post, 2009). At the beginning of 2012, the FBI tendered the development of an early-warning system based on open-source information from different social networks (BBC News, 2012). Beside Facebook, British police also target Bebo and MySpace to try to understand and to prevent teenage murders (Daily Mail, 2008).

3.2 Successful investigation on Facebook

**Picture database.** The police in Hamburg and Mecklenburg-Western Pomerania use public Facebook pictures to match them with pictures of prospective traffic offenders caught by a speed camera. This process is faster and more cost-efficient than identifying the driver personally. Two cases have been reported in which suspects could be freed from blame since their Facebook profile picture did not match the speed camera’s photo.

**Location identification.** In the following two cases, US police used Facebook to locate suspects. They were able to find and arrest a fugitive who had fled to Mexico. Via his Facebook friends, they accessed the man’s Facebook wall who regularly updated his profile with his current location (Stern, 2010). In a similar case, a suspect posted on his wall: “Catch me if you can, I'm in Brooklyn” (San Francisco Chronicle, 2011). The police located the computer the man had used and arrested him.

**Alibi.** A 19-year old man was accused of two robberies. He was on remand for 12 days and claimed to be at home during the time of the offence. After all, a Facebook message sent to his girlfriend one minute prior to the crime from his home computer could prove his innocence (Stern, 2009).
3.3 Problems of police investigations via Facebook

Information on Facebook can be distinguished between public and private information. The collection and use of public data by the German police do not conflict with the right for informational self-determination ensured by the Articles 2 (1) and 1 (1) GG (Grundgesetz; Basic Law), i.e. basically “The right of the individual to decide what information about himself should be communicated to others and under what circumstances” (Westin, 1970). The German Federal Constitutional Court (Bundesverfassungsgericht, 2008) confirmed that public authorities can use any public information on the Internet for their purposes. However, most of the information in online social networks cannot be accessed that easily. Most Facebook users disclose personal information and pictures only to friends (O’Brien and Torres, 2012), making it difficult for the police to collect the required data.

One possibility for the police to access private data is to approach Facebook directly. However, non-US police authorities struggle accessing data directly from Facebook, as the following case shows: a German judge asked Facebook for access to an accused man’s account. As the data is stored on US servers, his request was denied by both Facebook Germany and Europe who referred the judge to their headquarters. However, the US data protection laws forbid Facebook to provide data to non-US authorities if no official letter rogatory has been requested. As this request is a very time-consuming process (Spiegel, 2012b, Heise online, 2012c), it was not realised by the German judge.

The police can also use a covert or false identity to access private data, e.g. pretending to be part of the suspect’s network. It is judged critically to what extent communication in social networks is worthy of protection and thus not usable for undercover investigations. The German Federal Constitutional Court (Bundesverfassungsgericht, 2008) decided that (undercover) police investigations on the Internet usually do not conflict basic rights. When communicating on the Internet, an individual cannot assess for sure if the communication partner is who he pretends to be, and thus he cannot be sure that he does not interact with a public authority. However, the police must not exploit data that it would not have received otherwise. This means that the police can use, e.g. information somebody freely shared in an online forum, but not private information the police specifically asked for under a false name.

Table 2 summarises the main advantages and critical aspects of police investigations via Facebook.

<table>
<thead>
<tr>
<th>Advantages</th>
<th>Critical aspects</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information from public profiles (including a person’s recent picture, place of residence, occupation or friends) can easily be accessed and used without a legal restriction</td>
<td>Most Facebook members disclose personal information and pictures only to friends</td>
</tr>
<tr>
<td>US police can access private Facebook information, if an official decree is available</td>
<td>US data protection laws forbid Facebook to provide data to non-US authorities without an official letter rogatory</td>
</tr>
<tr>
<td>Facebook search software can efficiently crawl profiles and extract additional information</td>
<td>In Germany, information collected under covert or false identity can conflict with the right for informational self-determination (Articles 2 (1) and 1 (1) GG)</td>
</tr>
<tr>
<td>Data can be used to expose or to prevent criminal acts</td>
<td></td>
</tr>
</tbody>
</table>

Table 2. Advantages and critical aspects of investigations via Facebook

4 Outlook: Future Application of Facebook

In addition to publishing requests for information on the police’s own Facebook page and to access user information for investigation purposes, Facebook offers more functions the police could use in the future. In this chapter, we present three possible evolutions.

Biometric facial recognition. On average, a Facebook user displays 282 pictures (Statista, 2011). In June 2011, Facebook (2011b) started applying biometric facial recognition software. When a user uploads a new picture, it proposes which of his friends might be in the photo (ZDNet, 2011a). If the proposal is wrong, the user can manually enter the name of the person. This way, the facial
recognition software learns from the user. The police could apply Facebook as a picture database and use facial recognition to identify photographed people, e.g. in football stadiums or traffic controls.

European data protection authorities criticise Facebook for activating the face recognition function by default for all users without letting them know (ZDNet, 2011b). In Germany, such kind of storage and usage of biometric facial data is legal only if supported by law or with the user’s formal consent. Otherwise, it conflicts with the users’ right for informational self-determination. Thus, an irreproachable legal application for biometric data use by the German police is not given today. In September 2012, Facebook deactivated the function by default for all users in Europe (Zeit, 2012b) and finally deleted the data collected so far in February 2013 (Heute, 2013).

**Intelligent cameras.** The idea of “intelligent” cameras is to automatically recognise situations that require an intervention by policemen or guard staff, and to initiate the necessary next steps such as triggering an alarm. Ongoing research focuses on identifying violent-prone behaviour before it comes to an act by analysing a person’s gesture, facial expression and body movements (Courtney, 2011). In August 2012, New York police introduced an intelligent monitoring system for terror defence purposes which could also be used to fight common crime acts (Spiegel, 2012c). It links pictures from surveillance cameras with police databases, maps and the emergency call system (Heise online, 2012d). Some UK police cars have already been equipped with intelligent cameras linked to photo databases and facial recognition software.

**Cookies / analysing browsing habits.** Since April 2010, Facebook’s “Like” button is not only applied within the social network, but can be placed on every other website. 19.2% of the top 1 million websites worldwide already use the “Like” plug-in (Web Technology Surveys, 2012). Using cookies, Facebook collects data on websites its users visited and whether or not they clicked the “Like” button (ULD, 2010). Roosendaal (2010) discovered that Facebook does not only track its own users, but also non-Facebook users through all websites that implemented Facebook Connect. The collected data includes the IP address, the browser used, and installed software and is stored for two years (ULD, 2010). Facebook Connect’s successor Open Graph (Facebook, 2013e) expands Facebook’s social graph (i.e. link to friends and groups) to third-party services and collects information from its members on popular websites such as Spotify, Netflix, IMDb and many others. Altogether, this large amount of information may permit police authorities to match a suspect’s Facebook activity with his non-Facebook web activity, and thus to create an extensive profile of a suspect, including visited Internet pages, Facebook posts, messages and pictures very efficiently.

**5 Discussion and Conclusion**

Based on a comprehensive compilation of media reports, contributions from the European Union and the German federal government, as well as the study of existing laws and judiciary decisions, we examined the state-of-the-art police exploitation of the Facebook service. The main objective of the police’s Facebook use is to collect information that helps them to trace criminals and to solve cases or prevent criminal offences. Facebook data can be used by the police, e.g. to track the location of a suspect, get access to recent pictures or to interact with possible witnesses.

**Recommendations for policy makers.** The development of new information technologies, including social networks such as Facebook, is often much faster than the passage of appropriate laws. We
found that the exploitation of Facebook information can interfere with (innocent) people’s privacy and their right for informational self-determination. Creating a legal framework that protects personal rights, but enables the police to use Facebook information to prevent and solve crimes is a critical challenge that remains to be addressed by the respective working group of the ministry of justice. To achieve this, we have three concrete recommendations for policy makers which laws should be approached. First, there is no clear legislative in Germany that controls Facebook tracings. Appendix 2, Section 3.2 RiStBV is only a guideline for the police work, and is partly ignored (e.g. “Private websites should not be used.”). A consistent national information policy to determine which information can be published on Facebook (e.g. identikit pictures) is still missing. Second, a solution to simplify the collaboration between Facebook and European authorities needs to be found. As of now, an alignment of US and European data policies, or the data storage on European servers may enable non-US authorities to access private Facebook data more effectively to support investigations. This may be addressed in the near future by the European Cybercrime Centre (EC3), effective since the 1st of January 2013. As part of Europol, it promotes the fight against cybercrime in Europe and “pools expertise and information [and] supports criminal investigations” (European Union, 2012). Third, German data policies need to be updated to boost the efficiency of the police’s Facebook usage. The EU passed the Data Retention Directive in 2006 (2006/24/EG) which obliges Internet service providers to store Internet traffic and transaction data (including IP address, e-mails sent and web sites visited) for up to 24 months on supply, so law enforcement agencies can access it after a committed crime or if a terroristic threat exists (Nettleton and Watts, 2006). In Germany, the Directive has not been implemented yet as unsolved privacy issues still remain.

Avenues for future research. This paper shows several success cases of police work via Facebook, mainly taken from a six-month pilot project executed by Hanover police. There, Facebook information is already used successfully on a regular basis for tracing purposes. Nevertheless, academic literature on police tracings and investigations via social networks such as Facebook is still very scarce. Based on our findings, we will present hypotheses that provide avenues for future research.

Hypothesis 1: Tracings via Facebook are more effective than tracings via other media. Given the advantages of public tracings via Facebook (i.e. large audience, fast response rate, requests publishable at no costs), we assume that the social network is a very suitable channel to ask for the people’s help in finding witnesses and prospective offenders. It remains to be proven empirically if the effectiveness of requests for information on Facebook are superior to those published through other channels such as TV, radio or newspaper. A large-scale comparison of Facebook vs. non-Facebook tracings which covers the number of received indications and the average time until the traced individual or property have been found, could uncover the effectiveness of the different channels.

Hypothesis 2: Tracings via Facebook are more efficient than tracings via other media. We have seen that tracings via Facebook may not only be very effective, but also more efficient (in terms of time and money) than via other media. First, Facebook is a very fast response medium enables quick input for the investigative work. Second, Facebook tracings can be published without additional costs, unlike TV spots or printed posters. However, a higher number of objectionable posts may occur. An efficiency study that identifies to what extent a larger personnel expenditure compared to traditional channels is justified, would be insightful.

Hypothesis 3: Many Internet users feel uncomfortable regarding police tracings and investigations via Facebook. Information as requested and shared during police tracings and investigations are pretty sensible and not necessarily something a user expects to see or wants to share within a social network. Users may oppose to cooperate for different reasons, e.g. if they feel supervised by the police or mistrust Facebook’s data management. Behavioural studies, e.g. investigating how Facebook users feel about reading and possibly sharing sensitive information relevant to the police, can help to uncover findings that support the users’ acceptance for this channel and thus eventually improve the police’s communication policy and approaches.
References


Daily Mail (2008). Police target Facebook and Bebo to try to understand more about teen gang murders. www.dailymail.co.uk.


1All Internet references have been accessed 30th March 2013.


NDR (2012b). Wie sinnvoll ist die Facebook-Fahndung. Air date: 19th January 2012.


