ONLINE WITH THE PUBLIC

– HOW SMARTPHONES AND SOCIAL MEDIA ARE CREATING NEW OPPORTUNITIES FOR THE NORWEGIAN POLICE

ISBN 978-82-92447-68 – 0 (printed version)
ISBN 978-82-92447-69 – 7 (electronic version)

Report no. 2 2014
Published: Oslo, August 2014
Cover: Birgitte Blandhoel
Printed by: ILAS Grafisk
Published on: www.teknologiradet.no

FOREWORD

The Norwegian police are on the brink of an exciting new era. Weaknesses and shortcomings identified in the aftermath of the terrorist attacks on 22 July 2011 have provided us with a solid basis on which to shape the police of the future. The Norwegian police are currently undergoing a comprehensive and historically important reform process.

Society has changed drastically since the police last underwent such extensive changes. Today, three out of four people in Norway have a smartphone. We take them with us everywhere we go and use them to share text, photos and video – and not least communicate with each other via social media. (And of course sometimes even to make phone calls!).

This report discusses the possibilities this technology opens up in the field of emergency and disaster management. How can the network of citizens' smartphones be used to enhance the situational awareness of the police in the event of an emergency? Can we foster closer interaction between the police and the general public? What choices have to be made to maintain the balance between security and openness?

The expert group consisted of:

- *Gisle Hannemyr,* Lecturer, Department of Informatics, University of Oslo
- *Håkon Wium Lie,* CTO, Opera Software (and member of the Norwegian Board of Technology)
- *Silvija Seres,* CEO, Techno Rocks (and member of the Norwegian Board of Technology)
- *Inger Marie Sunde,* Professor, the Norwegian Police University College

The Norwegian Board of Technology's project managers Hilde Lovett and Robindra Prabhu headed the project, which was partially funded by the Ministry of Justice and Public Security.

The Norwegian Board of Technology is an independent body that advises the Norwegian Parliament and other authorities in key technology issues and promotes an open, public debate on important dilemmas. This report is the first in a series of three reports exploring how new technology may impact the future of police work and how these changes may challenge the boundaries between security and openness. We hope this report will contribute to an active, nuanced debate about the new opportunities available to the police.

Tore Tennøe
Director, The Norwegian Board of Technology

CONTENTS

1. SUMMARY AND RECOMMENDATIONS

Norwegians are world leaders in the use of smartphones and social media. However, the police do not currently make the most of this infrastructure. The public can be a source of detailed and up-to-date information that can enhance the police's situational awareness and provide a basis for making decisions in connection with accidents and crimes.

The Norwegian police are currently undergoing their most important and comprehensive modernisation process in recent times. Both the report of the 22 July Commission[1] and the Police Analysis[2] provide in-depth descriptions of the state of the Norwegian police, and both make it clear that better use of ICT and modern technology is an important "key to better emergency preparedness in the future".[3]

The Norwegian police force is now being transformed and equipped to meet future challenges, and documented weaknesses are being rectified. The "Reform Programme" (*Endringsprogrammet*) shall follow up on the improvement measures proposed in the wake of the terrorist attacks of 22 July 2011.

[1] Official Norwegian Report (NOU) 2012:14, "Report of the 22 July Commission"
[2] Official Norwegian Report (NOU) 2013:9, "One police – equipped to meet future challenges"
[3] Official Norwegian Report (NOU) 2012:14, "Report of the 22 July Commission", p. 455

The "Value Adding Programme" (*Merverdiprogrammet*) shall provide the Norwegian police force with the necessary ICT upgrades to make it a modern information organisation.

1.1 DIGITAL INTERACTION BETWEEN THE POLICE AND THE PUBLIC

The overall objective of the reform work is to ensure that the police are better equipped to perform their duties and to provide better police services to the public. At the same time, technology is changing the public's expectations of the police.

Within just a few short years, new technologies have revolutionised the way we communicate with one another. Smartphones have become indispensable for very many people, and social media have become an important arena for public debate. People communicate through photos, video and text. With this development comes an expectation that contact with the police can also take place via the technological tools we use on a daily basis, in a way that makes the most of the many possibilities technology affords.

This has implications for how the local police will communicate and interact with the public in the future. Today this kind of communication primarily takes place via voice calls. At the same time, citizens have never been better equipped to assist the police with important information, which in turn may result in:

- **Shorter response times,** through access to accurate positional data and timely information from the public.
- **Improved situational awareness,** through, for example, photos and video from the public, which may be especially useful to help improve the police's understanding of the situation before they arrive on the scene. This in turn provides **improved response quality** and better preconditions for good **collaboration and coordination** between the police and the emergency services.
- **Closer contact with the public** through a broader interface with the general public's everyday digital life.

Together smartphones and social media are major drivers of change in society and are giving rise to new sources of information that could greatly benefit the police. At the same time, the new possibilities must be weighed against the interests of privacy and the possible consequences for a free and open society. It will be crucial to draw boundaries for how far the police shall be allowed to go in their use of this kind of information.

This report aims to address a blind spot in the processes of change that have already been initiated and ensure that public participation is not overlooked as an important resource. At the same time the report seeks to constantly weigh the new opportunities up against the interests of transparency and privacy.

1.2 THE POLICE MUST HARNESS THE POTENTIAL OF CITIZENS' SMARTPHONES

People take their phones with them everywhere, and members of the public are often the first person on the scene of an incident. Smartphones are so much more than a telephone: they are computers with a range of different sensors. The public can thus supply the police with detailed digital information from the scene of an incident, in the form of, for example, photographs, video and text with precise information about time and location.

Digital emergency text messages and tips are a natural modernisation of the current voice-based emergency call system. Using modern technologies, the public can help improve the police's understanding of the situation and provide important information that might have been lost in a verbal description. At the same time, smartphones increase the possibilities for interaction between the police and the public, both before and after an incident has occurred

Digital information from smartphones can benefit the public in at least three different contexts:

- **"Precautionary":** The opportunity to voluntarily share precise location data with the emergency services gives citizens new ways to reduce risks to their own safety, both when they are alone (e.g. when hiking in the mountains) and when they are in crowded places.

- **"Call for help":** Once an accident has occurred, and speech is not possible or is difficult, smartphones enable communication via text, photos, video, etc. At the same time, important information such as location and health data can be submitted to the emergency services automatically.

- **"Eyewitness":** When members of the public witness an incident, photographs, video and audio recordings can quickly and easily document the situation and course of events.

When large crowds submit this kind of data, the total volume of information can be collated in a variety of ways to provide the police and emergency services with:

- rapid access to critical information
- a better and more accurate overview of the situation
- the possibility to map and follow developments as the incident unfolds and communicate with the citizens on the scene during the incident

Both on its own and in a broader context, information from the public can help improve situational awareness on site and as events unfold. Since most people use a smartphone in their everyday activities, it is both useful and important to connect this existing network of sensors to the emergency management systems of both the police and other emergency response agencies.

The Norwegian Board of Technology therefore recommends that arrangements are made to enable the public to submit digital emergency messages and tips in Norway, and that the police use digital information submitted by citizens in their work. This will entail some technical challenges and will also require clear guidelines for information management and use. It is important that new forms of interaction between the police and the public do not contribute to an unintended surveillance regime.

An emergency app should be developed for smartphones in Norway

The emergency services ought to offer a publicly available emergency application for smartphones and other mobile devices that makes it easy and safe for the public to report incidents to the emergency services. It must be possible to share precise location data, as well as communicate via voice, text, instant messaging, photographs and video. It should also be considered whether the application should be able to automatically submit profile data such as the person's name, medical information, next-of-kin and their contact details.

The police must be able to receive and process digital emergency messages and tips from the public, with information in the form of photos, video and GPS location, etc.

At present, all communication between the public and the emergency call centres is via voice calls. It is not currently possible to submit digital information such as photographs, video and GPS location to the emergency services in an emergency situation. At the same time, in a questionnaire survey the Norwegian Board of Technology found that 77 per cent of the respondents stated they would be willing to share photos and video from their mobile phone to improve situational awareness in connection with an incident.[4]

In order to ensure that both the police and the public are able to benefit from a public emergency app, it is important that the ongoing reform processes ensure that the new IT systems for the police and the emergency services are able to receive, process and use digital emergency messages and tips from the public.

The Ministry of Justice and Public Security has decided that emergency calls using text messaging (SMS) shall be introduced for the deaf and people with hearing impairments by the end of 2014, with the possibility to extend this service to the entire population. This emergency alert system will be linked to the construction of the new Public Safety Network ("Nødnettet").

While this kind of service is certainly a step in the right direction, the ambition must be to make much broader use of the many opportunities that citizens' smartphones open up for society's emergency preparedness work. This means that the emergency call centres must be equipped to receive, process and use other digital information from the public too, such as GPS location, photographs and video. It is important that the new Public Safety Network does not limit the opportunities for this kind of information sharing and collaboration between the police and the public in the long term.

[4] Questionnaire survey with 100 respondents aged 15 years and older conducted by Norstat in March 2014 on commission from the Norwegian Board of Technology to investigate public attitudes to communication and information sharing with the police via smartphones and social media.

The Ministry of Justice and Public Security ought to provide an account of how the new ICT solutions at the emergency services' call centres will be designed to support other forms of communication with the public than voice calls and SMS, such as chat, photos, video and audio recordings.

Systems to receive this kind of information must not only be regarded as an emergency alert service; they should also be considered as a system that provides the public with the opportunity to improve the situational awareness of the police through digital tips, when needs arise. It is important that the work on identifying which adaptations will be necessary is done as early as possible and is not postponed until after the new Public Safety Network has been completed.

Digital emergency messages and submission of tips must be free, accessible to all, and have priority in the network

It is important that new emergency alert services are made available to everyone and are universally designed so that they are accessible to all. Broad public accessibility is also essential for the police to be able to reap benefits in the form of improved situational awareness in connection with minor and major incidents.

Emergency calls using text messaging is to be introduced for the deaf and people with hearing impairments in Norway by the end of 2014. It is important that even such a minor extension of the emergency services is not only made available to deaf people and people with hearing impairments.[5] Digital communication with the emergency services through, for example, texts (SMS), chat, photographs and video is a useful service for everyone and ought therefore to be made available to the entire population.

In the same way as emergency calls are free of charge today, digital emergency messages and tips ought also to be free to send.[6] Digital emergency messages must also be given sufficient priority in the network.

The police must develop clear guidelines on how and for how long digital messages from the public can be used

[5] http://www.tv2.no/2014/06/11/nyheter/nodnett/5687506

[6] "It shall be possible to make calls to the emergency services' emergency call service free of charge and without the use of coins, cards, codes or other means of access." The Electronic Communications Act: http://www.lovdata.no/all/tl-20030704-083-002.html#2-6

Digital messages from the public are submitted voluntarily and contain private or "closed" information that is only intended for the police. At the same time, photographs and video may contain more information than the sender is aware of.

When the public is given the opportunity to send digital emergency messages and tips to the police, the police will be given access to a much richer pool of information than is currently the case. This kind of digital information will also be easier for computers to search, collate and analyse than the current voice calls from the public. In order for the police to be able to maintain a high level of public trust, it is essential to have clear guidelines for the use of the submitted information. These guidelines ought to be publicly available and answer the following questions:

- How is the content of distress messages and tips secured against unintentional use, both during submission and when saved?
- Which elements of a message are saved and for how long will they be archived?
- How can the messages be used and linked to other information, and for how long can this be done before the messages are deleted?
- How will surplus information be used?

Through this kind of open and transparent contract with the public, the police will be able to build public confidence that the privacy and legal rights of both the sender and the people that are identifiable in the distress messages are safeguarded.

1.3 SOCIAL MEDIA AS A SOURCE OF INFORMATION FOR THE POLICE

Norwegians are active users of social media. 80 per cent of the population state that they are a member of a social network[7], while 65 per cent of Norwegian Internet users state that they use social media every day.[8] Social network-

[7] TNS Gallup for the Norwegian Board of Technology and the Norwegian Data Protection Authority, January 2013

[8] The Norwegian media barometer 2013, Statistics Norway (2014)

ing sites are an increasingly important communication medium for people, including in the public exchange of opinions. As the terrorist attacks on 22 July 2011 also showed, information spreads rapidly on social media, and much of it is open to everyone – including the police.

Many commercial players have become aware of the opportunities inherent in social media, and new tools for the collection and analysis of large volumes of this kind of data are constantly being developed. This also opens up new opportunities for the police.

In connection with major and minor incidents, partially automated monitoring of social media could provide the police with valuable additional information that helps improve situational awareness. A marked increase in activity on social media may also signal that events are unfolding. In the Netherlands, the police have tested a tool that automatically scans large volumes of information on Twitter and uses algorithms to extract and sort information that may be relevant for the emergency services in connection with major incidents where citizens are often the first on the scene and up close to the events.[9]

Social media are not only a new source of information for the police, but also provide new opportunities for closer interaction with the public and to involve them in the police's work. Social media can also contribute to better understanding of how the public experience the police and of what they are concerned about.

Several police stations in Norway already use social media, albeit primarily as a channel to provide information to the public. The Norwegian Board of Technology recommends that the police's use of open social media be extended so that they are also used as an incoming channel for information and communication with the police.

At the same time, there must be clear objectives and guidelines for police activity in the open social media – to avoid an unfortunate chilling effect.

The police ought to monitor open information on social media

Automated computer programs that monitor information on social media provide a unique opportunity for early warning and improved situational

[9] http://www.newscientist.com/blogs/onepercent/2012/04/making-twitter-make-sense-for.html

awareness, especially in connection with major incidents. Along with digital emergency messages, tips from the public and the police's own field reports, information on social media can be a very important contribution to situational awareness and emergency management.

Initially, the police's surveillance and analysis ought to be limited to aggregated information on social media and not be used to identify individuals in the investigation. The purpose of the monitoring ought to be to improve situational awareness in connection with an incident and to chart the public's attitudes or feedback relating to the police's work.

This restriction may be reassessed when the police have accumulated sufficient experience and expertise in analysis and use of information on social media.

Furthermore, the police's use of social media ought to be expanded so these channels serve as a platform to involve citizens in the police's every-day work, especially local community tasks. This will pave the way for closer collaboration with the public, who in turn will be able to provide the police with more targeted information and feedback, when needs arise, both in connection with acute incidents and in the more long-term work.

The police must have clear guidelines to prevent a chilling effect

The police's monitoring of and presence on social media may be perceived as a barrier to people's freedom of expression on these channels.

It is therefore important that the police's every-day monitoring of social media only covers information that is publicly available for other social players, and that all monitoring activities are firmly rooted in a clearly defined distinction between open and closed information.

There are many different social media, which all operate in different ways. For example, tweets are accessible to anyone with Internet access, while Facebook requires log-in. Information may also be shared with everyone, many people or a select few, both deliberately and unwittingly. At the same time, general perceptions regarding the boundary between the public domain and the private domain in digital media are constantly changing.

To avoid the police's presence in social media resulting in an unwanted chilling effect that influences people's natural use of these media, it must be assessed where these distinctions are drawn, with a particular focus on the use of this kind of information in the justice sector.

Furthermore, it is important that the police's use of social media is anchored in a clear strategy for the entire organisation. The purpose of the police's use of social media must be clearly defined and must be followed up with unambiguous guidelines for proper use. The guidelines should answer the following questions and be openly shared with the public:

- Which social media are being monitored at any given time and for what purpose.
- The methods used in this monitoring, and an assessment of whether the relationship between the purpose and the methods is proportional and necessary.
- How and for how long collected information will be archived.
- How the information can be used and collated with other information.
- What editorial mechanisms the police use to protect people's privacy when citizens are actively involved in a case.

2. NEW OPPORTUNITIES FOR THE POLICE

"There is shooting on Utøya. My little sister is there and just called home."
Friday 22 July – 17:41:10. Ms. Tirill.

This was the first tweet from Utøya after the shooting started. The young people who were on Utøya while the shooting was going on sent text messages to family and friends, and even directly to government officials. They used social media to tell people about their own situation and to find out about others on the island.[10]

A good police response requires prompt, precise information from the scene of the incident. Members of the public are often the first on the scene, and most people take their smartphone with them everywhere they go. It is therefore highly probable that there will be one or more smartphones in the vicinity of most incidents. The public can send text, photographs, audio and video recordings from the scene. This is information that can help the police in their work, both on their way to the scene and in their subsequent follow-up of the situation.

[10] The 22 July Commission talked to 185 people who were on Utøya during the shooting about their use of social media in the first 24 hours after the terrorist attack. Of these, 37 stated that they were active on social media while the shooting was going on; Official Norwegian Report (NOU) 2012:14; Report of the 22 July Commission, p. 277

Citizens' smartphones are a resource that the police do not currently harness. Over the last few decades smartphones have given rise to a new situation, where people communicate and share information in entirely new ways. At the same time, advances in IT have made it easier to handle large volumes of data and undertake complex analyses using digital information. This report describes how these developments can change and strengthen the traditional interaction between the police and the public. Today, more than ever before, the public can be actively used as a resource to provide more police power. This may have major implications for how the police will work in the future.

At the same time as advances in technology are providing new opportunities, important questions are also being raised related to data privacy and transparency. It is important to define clear limits for how far the police shall be able to go in their exploitation of the new possibilities and to consider what other unintended consequences this new technology may have for individuals and society.

2.1 THE PUBLIC IS WILLING TO SHARE

Norwegians are willing to share information with the police. Some 63 per cent of us would be willing to submit photos and video from the scene of an incident, and a similar proportion would like to receive requests from the police for observations from the place where they happen to be. As many as 92 per cent would like to collaborate with the police to prevent crime, such as vandalism in their local neighbourhood.[11]

In a survey undertaken by the Norwegian Board of Technology in collaboration with the Norwegian Data Protection Authority, over 60 per cent of the respondents totally or partially agreed with the statement that both the police and the security authorities ought to be able to use open information from

[11] Iversen and Dahl (2010), *"Politi 2.0: Kan sosiale medier bidra til økt dialog og samhandling mellom politi og publikum?" [Police 2.0. Can social media help increase dialogue and collaboration between the police and the public?]*, p 11

social media, blogs and other Internet services for prevention and investigation, while almost 20 per cent totally or partially disagreed.[12]

In connection with the work on this report, the Norwegian Board of Technology conducted a survey among 1,000 respondents aged 15 years and older to investigate public attitudes to communication and information sharing with the police through smartphones and social media. The survey confirmed the public's willingness to share information with the police, but also revealed that the public's attitude towards police presence on and use of social media is somewhat more nuanced. The results of the survey are presented in graphs throughout this report.

2.2 POLITICAL TOPICALITY

The Norwegian police are currently undergoing a rapid and comprehensive reform process. The terrorist attacks on 22 July 2011 served to accelerate this process. The reforms include changes in everything from structure and organisation to use of technology and upgrading of tools and methods. Several ongoing and upcoming projects will stake out the path for the police of the future.

At the same time, the information revolution and digitisation have changed Norwegian society in fundamental ways. These developments have transformed work processes in many different information-based activities in recent years. Policing is an information-intensive business, and it is both natural and necessary to consider how these changes will provide the police with new opportunities and challenges in coming years.

2.2.1 THE 22 JULY COMMISSION

The report of the 22 July Commission provided a detailed snapshot of the current state of the Norwegian police. An important message of the report was that the potential of modern ICT was not being exploited sufficiently[13] and

[12] Survey undertaken in conjunction with the International Data Privacy Day 2014. The survey was conducted by Opinion Perduco via a web panel in November 2013. A total of 1,501 citizens aged 15 years and older participated in the survey.

[13] Official Norwegian Report (NOU) 2012:14, Report of the 22 July Commission, p. 16

that we are in the middle of a technological revolution that the Norwegian police must embrace.[14]

The Commission also acknowledged that technology has changed the interaction between the police and the public: knowledge about the attacks spread rapidly to large parts of the population via mobile phones and social media. It also pointed out that we are now facing a completely new and interesting situation, where, for example, government officials receive information directly from victims via text message, phone calls and social media while a national crisis is ongoing and needs to be handled[15].

As an extension of this, the Commission sketched the outlines of the new sphere of opportunities that smartphones and other devices are opening up for the police, without going into detail about what this means and what consequences it will have for the police and society:

> *"Mobile phones and smartphones also offer photo and video capacity that the police will clearly be able to make use of, by establishing systems and software that can interact with the technology."*[16]

2.2.2 THE POLICE ANALYSIS

The Police Analysis[17] provides a thorough, comprehensive and well-documented analysis of the organisation, management and practices of the Norwegian police. This report too put technology and use of technology on the agenda. The Police Analysis discussed important issues relating to the organisation and management of ICT in the police in depth.

Proximity and accessibility to the public is a recurrent theme in the Police Analysis, but in this context technology is primarily discussed as a support tool that could improve efficiency in the performance of duties. Various information and self-service systems, such as for example electronic processing of applications and the possibility to book an appointment online, were cited as examples of how technology could facilitate contact with citizens.

[14] Official Norwegian Report (NOU) 2012:14, Report of the 22 July Commission, p. 336
[15] Official Norwegian Report (NOU) 2012:14, Report of the 22 July Commission, p. 454
[16] Official Norwegian Report (NOU) 2012:14, Report of the 22 July Commission, p. 336
[17] Official Norwegian Report (NOU) 2013:9, One police – equipped to meet future challenges

In this respect, the Police Analysis does not follow up on the parts of the 22 July Commission's report that describe the wealth of possibilities that smartphones, social media and new sources of information represent for the police. This is a weakness in the Police Analysis that the current report seeks to remedy.

2.2.3 RECOMMENDATION FROM THE STANDING COMMITTEE ON JUSTICE CONCERNING THE WHITE PAPER ON TERRORISM PREPAREDNESS

In the white paper Report no. 21 to the Storting (2012–2013) *Preparedness for terrorism*[18] the Stoltenberg Government provides an account of its follow-up of the 22 July Commission's report. Here the prevalence of mobile devices among the public and social media were primarily discussed as means for radicalisation and planning acts of terrorism. The possibilities they afford for new forms of interaction between the police and the public were not explored.

The Storting's Standing Committee on Justice touches upon these deficiencies in Recommendation no. 425 to the Storting, 6 June 2013.[19] A unanimous committee "highlights the possibilities for using location information, photographs and video from citizens in emergency situations and in connection with emergency messages. The Committee believes that in a crisis situation it is important to have information systems that can quickly provide the most accurate, comprehensive and complete situational awareness."[20]

This report aims to map and clarify these new opportunities, and at the same time discuss challenges related to the advances in technology.

2.3 OBJECTIVES AND DELIMITATIONS OF THIS REPORT

This year the Norwegian Board of Technology is publishing three reports on developments in society and technology over the last decade that have changed the preconditions for the police's work.

[18] Report no. 21 to the Storting (2012–2013), Preparedness for terrorism – Follow-up of Official Norwegian Report (NOU) 2012:14 Report of the 22 July Commission

[19] Recommendation no. 425 to the Storting (2012–2013), Recommendation from the Standing Committee on Justice concerning preparedness for terrorism, 6 June 2013

[20] Recommendation no. 425 to the Storting (2012–2013), Recommendation from the Standing Committee on Justice concerning preparedness for terrorism, 6 June 2013, p. 17

2.3.1 THREE REPORTS ON TECHNOLOGY IN THE POLICE

The current report is the first in the series and addresses two main topics:

1. Smartphones and the opportunities they represent for interaction with the public.
2. How information from new, open sources, and especially social media, can be used to improve the police's situational awareness as an incident unfolds.

The second report will examine how predictive analysis methods can be used to forecast where and when crimes will take place, and how they can support the police's prevention work.

The last report in the series is about how technology for information sharing can facilitate that the police receive the necessary, accurate and adapted information at the right place and at the right time.

The Norwegian Board of Technology's conclusions build on experiences from other countries and an analysis of how the main technological developments will affect the police's working methods in the future.

2.3.2 DELIMITATIONS

This report examines how the prevalence of smartphones and other mobile devices among the public in Norway can provide the police with the opportunity to obtain information from the scene of an incident and the surroundings as events unfold. It aims primarily to describe the new possibilities for interaction between the police and the public. The report will not discuss the requirements related to the technical infrastructure necessary to realise these opportunities in any depth.

Moreover the report is primarily concerned with the police's *operational* activities, which are both broad and diverse. In the broadest sense, this involves everything from prevention and intelligence to keeping the order, traffic management, operations control rooms, and rescue and emergency response work. In preparing this report, we therefore made a number of delimitations. The report does not consider technologies and collection of information that support police investigations and criminal proceedings or intelligence work, which typically falls under the Police Security Service (PST).

Prevention, intelligence, emergency preparedness, crime-fighting and investigation are, however, overlapping activities to varying degrees. Several elements covered in this report will therefore both be relevant for other operational areas in the police and constitute necessary prerequisites for harnessing the potential entailed by new and future technologies.

3. DIGITAL EMERGENCY MESSAGES AND TIPS

A smartphone is not just a telephone. Indeed, making a phone call is now only the fifth most used function on mobile phones (after Internet access and social media).[21] Smartphones are advanced computers with a variety of sensors that can share data over the Internet. They have a camera and microphone that allow people to record their surroundings precisely with the exact time and location, using text, photo, audio and video recordings. GPS and accelerometers can be used for precise positioning and to measure movement.

Today, three-quarters of people living in Norway have a smartphone.[22] And while, unsurprisingly, the younger segment of the population has been quickest to embrace smartphones, Figure 1 shows that smartphone prevalence is now increasing in the older age segments too.[23]

In practice this means that wherever there are people, there will also be small, sophisticated computers with a range of sensors in the form of smartphones. In this way, the public can be regarded as a network of sensors that can actively or passively contribute information to support the police's operational activities.

[21] Shane Richmond, "Smartphones hardly used for calls", The Telegraph, 29 June 2012

[22] MedieNorge and TNS Gallup, http://www.medienorge.uib.no/statistikk/medium/ikt

[23] Google, "Our Mobile Planet", http://www.thinkwithgoogle.com/mobileplanet

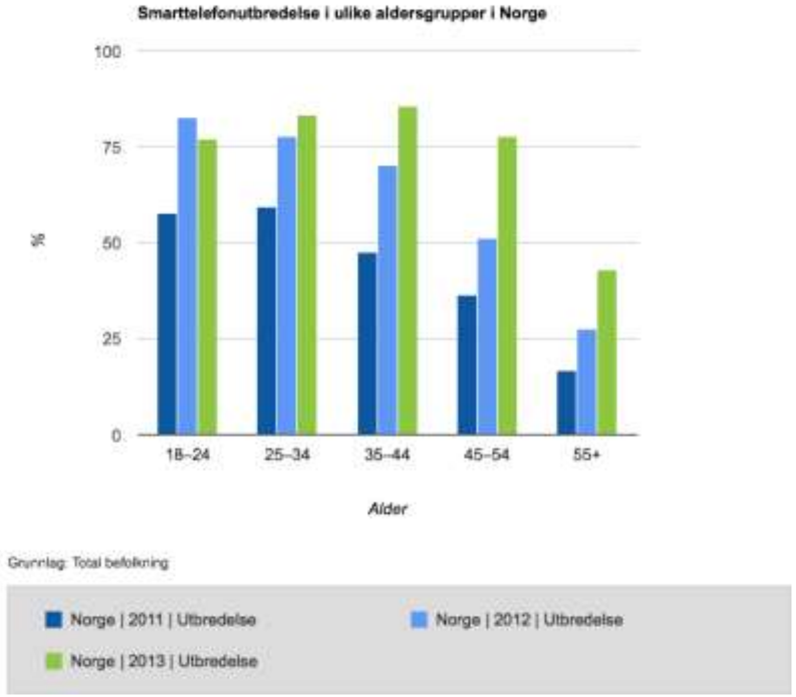


Figure 1 Mobile prevalence among different age groups in the Norwegian population from 2011 to 2013 (Source: "Our Mobile Planet", http://think.withgoogle.com/mobileplanet/).

This kind of data from citizens can be useful to the police in several different ways. Among other things, they can help ensure that the police have rapid access to:

- more detailed information via photographs and video, ensuring enhanced situational awareness
- precise positioning data and the ability to locate people when necessary
- better overview of an incident, by compiling photos from several people
- better understanding of the course of events and the situation in connection with a major incident or disaster
- knowledge about the movement patterns of large crowds

Because the information is digital, it can be processed and collated with other emergency messages in the police's computer systems. The police will be able to save valuable time that is currently spent manually registering and interpreting information in emergency messages. It will also help lessen the likelihood of errors and important information being overlooked. Partially automated processes can ensure that information is processed, sorted, analysed and shared among the relevant units in the police without loss of meaning. In this way, the information can be useful and actionable for the operations control room, patrols and police station alike.

To facilitate this kind of information collection and for the police to be able to handle this wealth of information properly, the police will have to start using new tools and methods and develop new guidelines for use. At the same time, this kind of rich pool of information raises some important and interesting questions relating to data privacy, transparency and how much we want the police to be able to know or find out about us at any given time.

Both the opportunities and the considerations that must be taken into account are discussed below.

3.1 ENHANCED SITUATIONAL AWARENESS

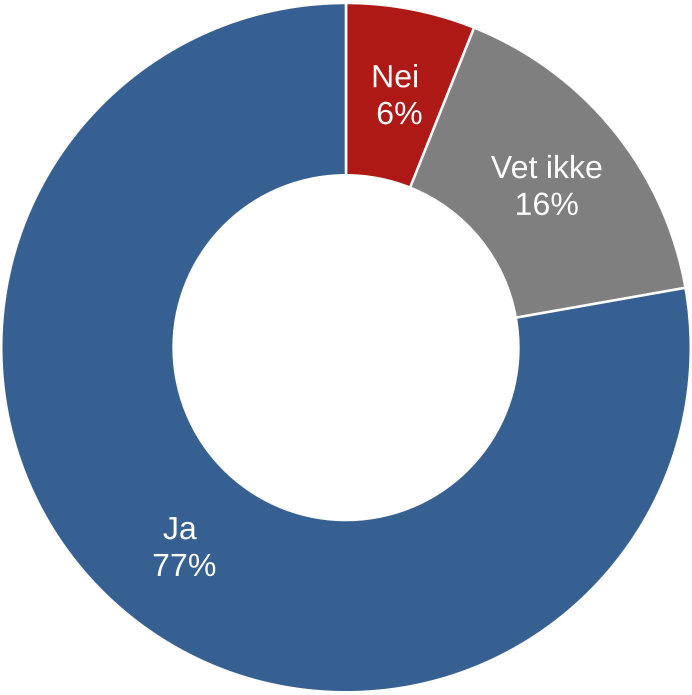
Access to relevant information from the scene of an incident is essential to establish correct situational awareness – a common understanding of what is happening, when it is happening, where it is happening, who is involved, what risks it entails for emergency teams and citizens, how the situation might develop, etc.

Smartphones provide an opportunity to improve the police's situational awareness before, during and immediately after an incident. Below are a number of examples of how citizens can provide the police with a better description of the actual circumstances.

3.1.1 DIGITAL PHOTOGRAPHS: MORE INFORMATION

The police can often read more from a photograph than an eyewitness is able to tell the traditional emergency call centre. A witness's description may be inaccurate or omit important details. Experience also shows that stress in connection with serious incidents means that many eyewitnesses forget important information such as the colour of a jacket or a car fairly shortly afterwards.

Would you be willing to submit photographs or video from your mobile phone to the police to help them to understand the situation better, if you witnessed a crime or were on the scene before them?



A digital photograph or video can be "stamped" with the exact time and place. Time and location information can be used to sort pictures taken at the same place and at the same time. As this is digital information, computers simplify the sorting process considerably. Relevant digital photographs and film clips can be shared rapidly and efficiently with all the parties involved, for example, in connection with a rescue operation.

Citizens now have the opportunity to document incidents and circumstances using on-site digital photography and video. In many cases this will be an important information resource for the police.

3.1.2 PHOTO COLLAGE: BETTER OVERVIEW

When the police receive several photographs from a single incident, these are collated to form collages, which help give a better overview of the situation. Computer image processing can be used to sort and analyse the photographs.

We saw an example of this in the aftermath of the Boston Marathon bombings in April 2013. Shortly after the explosions, the FBI and Boston Police Department initiated an investigation process based partly on "crowdsourcing", whereby citizens voluntarily contributed large volumes of digital information. The police were looking for clues as to who might have placed the bombs near the finish line and asked the public and neighbouring businesses to submit any photographs, videos and other descriptions of the finish line area immediately before and after the explosions. At the request of the police, citizens could also send text messages and start a dialogue with the police. The tips service is anonymous, a factor that the police in Boston regard as crucial to receive critical information.

The police received over 2,000 tips immediately after the attack. Thousands of photographs and videos from public and private surveillance cameras were stitched together with pictures from citizens' mobile phones. In this way the police were able to create a photo collage that drew a general and clearer picture of the scene of the incident and surrounding areas from many different angles. The police themselves have stated that this help was invaluable.[24]

Various digital information fragments from citizens can thus be stitched together to form a more comprehensive picture of a situation. Because the vast

[24] Conversation with the Boston Police Department

majority of the population have a smartphone, citizens can be involved in and contribute to improving the police's situational awareness through "information crowdsourcing".

3.1.3 GPS: PRECISE POSITIONING

The precise location of the caller is essential for the police to be able to assess the request and plan a suitable response, especially if the caller has been involved in an accident, witnessed an incident or is located in a high-risk area. Knowledge about the caller's location may also be useful if the police want additional information, such as photographs or video, to improve their situational awareness.

Under the current system, the whereabouts of anyone who calls an emergency phone number in Norway is automatically identified. If you call from a landline, the address you are calling from is identified. If the call is from a mobile phone, the approximate geographical position is worked out from the base stations in the vicinity.

A smartphone with GPS will be able to provide a more precise location than the caller's position calculated on the basis of nearby base stations. In good conditions, the location of a smartphone can be identified with an accuracy of approximately 7 metres or less.[25] (In less ideal conditions, such as in densely populated urban areas, it will be possible to specify the location with an accuracy of approximately 40–100 metres).

The police in Iceland have created a tracking application for smartphones. The application enables citizens to voluntarily share their GPS location with the Icelandic emergency services (112), which only stores the last five positions. If an emergency arises, you can alert the emergency services with a single keystroke using the application. The coordinates are used as the starting point to be able to guide people who have got lost or to initiate a search if necessary. In many cases the police have not had to send out a search party, thus saving considerable police resources, at the same time as the lost person has been brought to safety more quickly. With a little guidance, the missing persons have often been able to find their own way back. The Icelandic authorities plan

[25] http://no.wikipedia.org/wiki/Gps

to expand this solution to also include the opportunity to send multimedia messages.[26]

Digital information from citizens' smartphones can easily be labelled with very precise location information. Precise location data will not only help to reduce the response time; response quality will also be improved when the police have prompt access to precise location data and can extract necessary additional information and make the necessary preparations in advance. Moreover, experience from Iceland shows that such data opens up new and interesting ways to deliver services to the public.

3.1.4 MAPPING: UNDERSTANDING THE COURSE OF EVENTS

Groups of messages with information about the place they were sent from can benefit the police in other ways too. These kinds of messages can be counted, grouped and plotted on a map where they together form a series of snapshots from a course of events. For example, they can show how many people are in the immediate vicinity of an incident.

A smartphone will automatically be able to label digital messages with the precise time and location. New messages and updates will therefore be able to show how a situation evolves over time. By plotting emergency messages on a map, the police and emergency services are more easily able to prioritise their resources appropriately and adapt their response to the incident.

Haiti suffered a massive earthquake in January 2010. Many people were feared dead. People posted messages on social media describing the devastation where they were or asking for help. A special SMS code was set up for the public to be able to submit information about the greatest needs. Volunteers and charities went through the messages, identifying and locating the most acute "life-and-death" text messages, which they then plotted on a digital map. The map was used to prioritise efforts and send aid to the places where the needs were greatest. The aid agencies in Haiti reported that this map was invaluable in the search and rescue operation after the earthquake and that it helped save hundreds of lives.[27]

[26] Presentation: "The 112-app", Tómas Gíslason; deputy CEO of 112 Iceland + conversation with the Icelandic police

[27] http://newswatch.nationalgeographic.com/2012/07/02/crisis-mapping-haiti/

In Haiti much of the processing of the messages was done manually, so it took a relatively long time to plot all the messages on the map. Digital tools will be able to group and plot all emergency messages on a map automatically and in real time. These kinds of maps can also be enriched with information from social media. The police will thus be able to have immediate access to this overview and will not have to spend valuable time and resources on preparing the map.

In this way digital information from citizens enables prompt mapping of the unfolding of events. This may be very useful in response planning, collaboration and coordination between the emergency services.

3.1.5 MOVEMENT OF LARGE CROWDS

Knowledge about the movement pattern of large crowds can also be useful for the police. For example, it can make contingency planning and work in connection with major events such as concerts, sporting events, national celebrations (such as Norway's 17th May parades) and demonstrations better and more efficient.

New technology significantly improves the opportunities for collecting this kind of information. For example, when a smartphone reports its location at regular intervals, this information can be used to draw a picture of the movement pattern of the person using the phone. When many people share their location via their smartphone, this could provide useful insight into the systems and mechanisms of large crowds.

One example is the mobile application Waze, which uses location information from millions of motorists' smartphones to provide users with up-to-date traffic information in real time and suggestions for alternative routes. In terms of humanitarian aid, movement patterns from mobile phones have been used to map the spread of disease in the population.[28]

The London Metropolitan Police offers the public a mobile application for sharing information between the public and the police. They have since further developed the application to include the ability to share the mobile phone's location and direction of movement. The user must accept that this kind of data is sent anonymously at regular intervals for a limited period of

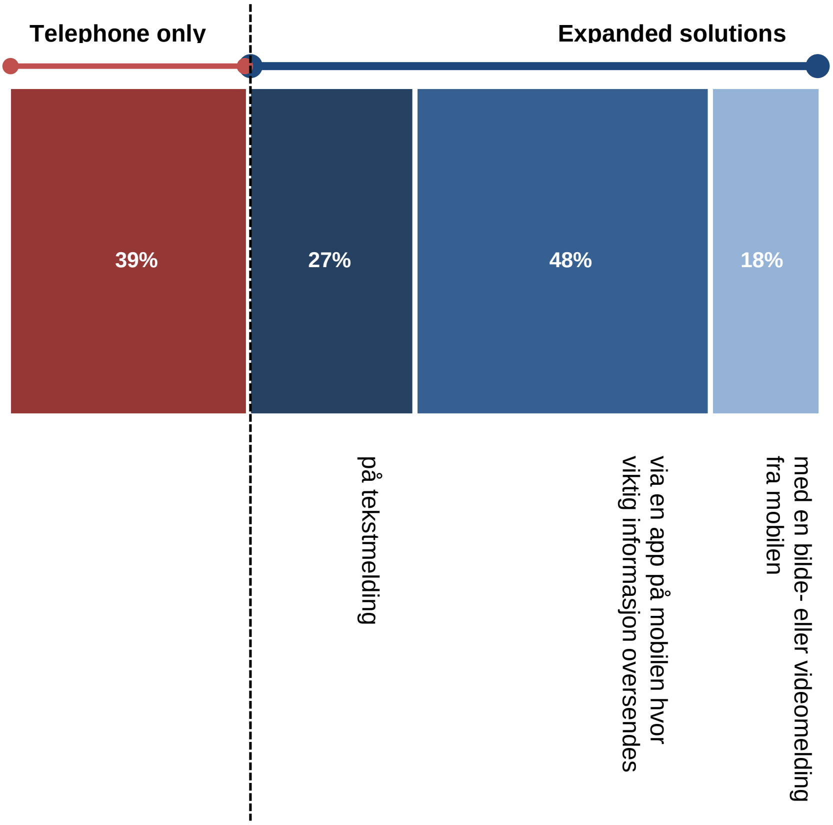
[28] "Mobile Phone Network Data for Development", United Nations Global Pulse, October 2003

time, usually before, during and after a scheduled event. The data are immediately logged on a map that shows where people have gathered and how the crowds are moving in real time.[29]

Anonymous location data from members of the public can thus be used to plot crowd movement patterns in real time and adjust the planned contingency measures accordingly. The example from London shows how this paves the way for new forms of collaboration between the police and the public.

[29] http://www.cityoflondon.police.uk/contact-city-police/smartphone-app/Pages/default

Imagine you are in a situation where you need immediate help from the emergency services. Would you like to be able to contact the emergency services in ways other than by making a traditional phone call?



3.2 NEW INTERACTION BETWEEN THE POLICE AND THE PUBLIC

The above examples show how smartphones provide the public with entirely new ways of reporting incidents and assisting the police with useful information from the scene of an incident as it unfolds. In many ways smartphones can be regarded as a platform for new forms of interaction between the police and citizens.

Digital information from smartphones can benefit the public in at least three different contexts:

- **Precautionary**: In the same way that people can choose to install a private burglar alarm, the examples from Iceland and London demonstrate new ways in which citizens can use their smartphone to reduce risk and possibly safeguard themselves against a future accident, for example by sharing positioning data.

- **Call for help**: Once an accident has occurred, a smartphone enables people to communicate with the police and the emergency services in many different ways, such as voice call, text, photographs and video. In an acute emergency situation, vital information such as location and health data may occasionally be transmitted to the emergency services automatically. This can save valuable time and ensure the safety of the person submitting the emergency message.

- **Eyewitness**: While the public can currently help the police by calling the police tips hotline or sending a written message via the Internet, smartphones mean they can also submit valuable information in the form of photographs, video and audio recordings, etc. Because most people have their phone on them at most times, these kinds of tips can be submitted live from the scene of an incident and be updated as the situation changes. For example, citizens can describe the way a fire in a building is developing while the emergency services are on their way.

Information from citizens' smartphones can benefit the police in terms of:

- **Improved situational awareness** through a larger pool of richer information. When many people submit information, this can significantly improve the police's situational awareness.

- **Faster and more precise resource management** through more detailed knowledge of both the scene of the incident and the course of events. This also provides the police with the opportunity to monitor events in real time and adapt and manage the resources as needs dictate.

- **Closer contact with the public** by citizens having easy access to the police at all times. This also enables electronic dialogue with people on the scene of an incident in real time.

Citizens' smartphones are thus not only a source of information for the police and a communication tool for the public; they are also helping pave the way for new and closer interaction between the police and the public:

- The police will be able to use citizens more actively as a resource to provide more police power ahead of an incident or when an accident has occurred.

- The public will experience the police as more accessible and close. Being able to get in touch with the police easily and rapidly will in turn lead to greater public involvement and trust.

In connection with the modernisation of the police's interface with the public, it is therefore essential that this is not limited to the development of online information and self-service facilities, or mere upgrades of the existing reporting practice (such as the opportunity to send emergency messages by SMS). It is crucial to think broadly about what role the public should play in the future of policing.

3.3 NORWAY'S EMERGENCY NUMBER 112 AS AN APP: A NEW INTERFACE WITH THE PUBLIC

The public must be easily able to communicate with the police in the ways and using the tools that they otherwise use in their everyday lives. At the same time, citizens equipped with smartphones constitute a valuable resource that the police must be able to draw on when necessary.

It is important to have systems in place that make it easy and safe for people to be able to send messages containing photographs, video and other information to the police. When needs dictate, the police must also be able to ask the public to submit relevant digital information and otherwise be able to receive these kinds of messages and process them efficiently.

Country / region	Functionality
Denmark	Precise location data is automatically sent when an emergency call is made.
Iceland	The application sends precise GPS coordinates to the emergency service's control room by SMS when an emergency call is made. The user can at any time choose to share their last five locations with the emergency services.
The Netherlands	Photographs and video can be sent to the police via an online form linked to the police's website (www.politie.nl), which is accessible via the application.
Catalonia	Users can receive information about ongoing emergency situations and location-customised instructions on what to do in the specific situation. The application provides coordinated access to traffic information, weather data, public transport information, etc.
The Canary Islands	Precise location data is transmitted, and emergency calls can be made via voice, text (instant messaging) and photographs. Medical profile data such as blood type and information about chronic diseases is transmitted automatically.
Lombardia	Precise location data is transmitted, along with the sender's personal profile and contact list.

Table 1 Countries and regions that have developed applications for contact with emergency services with extended functionality

3.3.1 ADAPTATION FOR SMARTPHONES

Mobile applications (or "apps") make it easy for smartphone users to send digital messages to the police, both in an acute emergency situation and in connection with eyewitness descriptions or tips. As Table 1 shows, the police and emergency services in several countries and regions have launched applications that in different ways exploit the possibilities afforded by smartphones. These kinds of mobile applications will usually take the form of a platform that provides access to a variety of functions on the smartphone, including voice, SMS, MMS, camera and recording equipment, GPS and chat / instant messaging.

In addition, these kinds of mobile apps will access information such as:

- the sender's name, address and national identity number
- age and main health data
- name and contact number of next-of-kin, etc.

The application can also extract information about the time, location and any direction of movement directly from the smartphone's systems. If desired, this information can be automatically transmitted to the police and emergency services with the emergency message or voice call. At the same time, it ought to be possible for the public to submit completely anonymous emergency messages, as discussed below.

The actual emergency message or tip can be formulated in different ways, depending on the sender's situation:

- the message may be recorded as a voice message, with or without video
- the message may be written as a text message, with or without photographs
- the message may consist of a predefined text, where the sender simply selects the relevant category and an appropriate description and attaches photographs or other information.

Smartphones allow people to send information to the emergency services over the mobile network (voice, SMS, MMS), mobile broadband or the Internet (VoIP, chat / instant messaging, photos, video, etc.). Different features of the mobile phone will use different communication protocols, and depending on coverage and availability, the mobile app may be able to switch between these different infrastructures. For example, if mobile broadband coverage is poor, a photograph could be compressed and sent over the mobile network as an MMS.

Once the message has been sent, the user will be able to receive confirmation via the app that the message has been received. The sender will also be able to receive any status updates from the police, such as "Units are expected to be on the scene in about 12 minutes" or "maintain a minimum distance of 100 m from the building".

3.3.2 PAST AND ONGOING INITIATIVES IN THE POLICE

The police have previously (in 2010) attempted to introduce a system for the reception of SMS emergency messages from the public. This initiative never got off the ground due to the lack of support for it in the organisation and the operations control rooms. Another problem was the lack of clear guidelines for the use and processing of the data received, and the implementation of new work processes and tasks.[30] To avoid the same pitfalls, it will be important to ensure that there is adequate support for the new system and that the necessary guidelines and training are in place.

West Finnmark Police District has successfully developed a prototype for a mobile app that allows users to order a new passport, report a case or chat with the police via their phone or tablet. It also allows citizens to submit photos and tips to the police and express any dissatisfaction with the police's work. The service is called "nødchat" (literally: "emergency chat"). However, the National Police Directorate has halted the further development of this app. The National Police Directorate is currently working on a centralised solution that facilitates mobile solutions and has requested that no local systems be initiated; instead the police districts must wait for the new central solution.[31]

On commission from the Ministry of Justice and Public Security, the Directorate for Civil Protection and Emergency Planning (DSB) has headed a working group that has studied the various alternatives for a future text-based service for the emergency control rooms, to enable the deaf, people with hearing impairments and people with speech impairments to communicate directly with the emergency services (2013). The working group acknowledges that smartphones open up interesting opportunities for digital communication between the public and the emergency services, but nevertheless recommend that priority be given to an SMS-based solution to begin with. It recommends that this be included as part of the delivery of the new Public Safety Network and the associated upgrade of the emergency services' control rooms and be

[30] http://www.aftenposten.no/nyheter/iriks/Stanset-SMS-nodmeldinger-i-2010-7268767.html#.UgTPRLzhX6w

[31] http://www.nrk.no/nordnytt/tommelen-ned-for-politi-app-1.11352077 and http://www.nrk.no/nordnytt/tester-ut-ny-politi-app-1.11182558

ready for implementation by the end of 2014.[32] The working group recommends that support for other forms of digital communication such as photographs, video, e-mail, chat / IM and apps should not be assessed until the new Public Safety Network is up and running, it has been ascertained that the SMS service is secure and efficient to use, and mobile coverage in Norway has been improved.

The introduction of an SMS-based solution is certainly a step in the right direction, but because such a large proportion of the Norwegian population already uses a smartphone on a daily basis, and in light of the communication possibilities smartphones afford, the Norwegian Board of Technology nevertheless holds that the plans for modernisation of the emergency and tips telephone service ought to be more ambitious. The emergency call centres' public services must reflect the current technological possibilities and enable people in distress to use the form of communication that they perceive as most appropriate. At the same time, the upgrade process must be followed up by reflection on how citizens' smartphones can be incorporated into the operational activities of the police as a resource that provides the police with more police power.

A mobile application ought therefore to be developed in parallel with the introduction of SMS-based notification and ought not to be postponed until the new Public Safety Network has been completed.

3.4 MANAGING THE FLOOD OF INFORMATION

3.4.1 WILL THE POLICE BE ABLE TO RECEIVE AND USE THE INFORMATION?

It will be a challenge for the police to be able to receive large numbers of digital emergency messages and effectively identify and process the important and critical emergency messages. The volume of information sent to the operations control rooms is already very large at times, especially in connection with major incidents. Another serious challenge is that people misuse the emergency number. Of the 14,000 calls to the emergency number 112 in Oslo each

[32] http://www.tv2.no/2014/06/11/nyheter/nodnett/5687506

month, 80% are stopped at the switchboard because they are not genuine emergency calls.[33]

The low threshold for sending digital messages may lead to the submission of large volumes of messages to the police, and it is reasonable to assume that many of them too will be hoax and false emergency messages.

A key advantage of digital emergency messages is precisely that they are digital and can thus be routed straight into the police's other information systems. Computers and digital tools can be used to automatically process messages without loss of meaning. This requires that the police establish the necessary processes, have the necessary analytical tools and undergo proper training in order to be able to receive and process digital emergency messages.

"The post-it note"

At 15.34.50 on 22 July 2011 someone phoned the Operations Control Room in Oslo to report an eyewitness observation. The witness had noticed an armed man wearing police uniform and could describe the vehicle. The report was written down on a post-it note. This note was ignored until 15.56, when it was further processed and the witness was called back. The information from this witness was compared with other information from the Government Quarter's security centre. The person who called the witness back was sure that the person in the vehicle had something to do with the explosion. She therefore flagged the notification as "important" in the operations log and took the necessary steps to ensure that the information was available to everyone.[34]

If this eyewitness observation had been digitised, it would have been easier for the systems to ensure it was not overlooked or lost in such a stressful situation.

Digital emergency messages can make the process of receiving, processing and sharing situational awareness information faster and easier, and reduce the degree of error. The possibilities to simplify the processing of digital emergency messages lie in the computer tools, which can do the following:

- Index and rank emergency messages by relevance, so that important information will always appear first, while hoax and false emergency

[33] http://dittoslo.no/indre-by/nyheter-indre-by/hadde-problemer-med-lyden-pa-tv-en-ringte-politiets-nodnummer-1.7901975
[34] Official Norwegian Report (NOU) 2012:14, Report of the 22 July Commission, p. 100

messages are given lower priority or are hidden altogether. This is similar to how a Google search works.

- Collate and compare information in emergency messages with information from other registers so that additional, relevant information can quickly be identified.

- Incorporate critical information into the situational awareness so that it can be shared with all the relevant patrols and units during an operation once it has been classified as relevant and important.

Tools that process digital emergency messages can quickly provide all the parties involved with access to critical information, improve the understanding of the situation, and at the same time reduce the likelihood of the message being overlooked.

LEEDIR: New service provides the police with prompt access to photos and video from citizens' smartphones

The Los Angeles Sheriff's Department has teamed up with the companies CitizenGlobal and Amazon Web Services to develop an image and video database that the police and emergency services can activate in a major crisis. LEEDIR (Large Emergency Event Digital Information Respository) is a cloud-based service that the police can easily activate when necessary.

Once the service is activated, the public is notified via an app on their smartphones and requested to submit photographs and video to the database. Information can be submitted anonymously. As the volume of data grows, the database expands automatically. The service can handle numerous different file formats, meaning people can submit large files when necessary, and also provides the police with a user interface where they can:

- Comment on and organise the images and videos they receive. The tool also makes it easy to extract additional information linked to the data, such as geographical position and contact information, if this information has been made available.

- Communicate and collaborate with other analysts taking part in the operation, as well as share certain data with collaborating emergency services and other players involved in the response.

In this way the service rapidly provides the police with an interface for contact with citizens who are at the scene of the incident and can document the course of events with their smartphones.

3.4.2 DOES THE NETWORK HAVE SUFFICIENT CAPACITY?

When an emergency arises, there will generally be many people who want to communicate. The network can quickly become overloaded. It is precisely in this kind of situation that it will be crucial that citizens can contact the police and other emergency services – via both voice-based emergency calls and digital emergency messages.

Very many emergency calls were made immediately after the shooting on Utøya started. Despite the high number of emergency calls, the emergency number constituted a small part of the overall telecommunications traffic in the area – at its peak just under 5 per cent.[35]

The Norwegian Post and Telecommunications Authority has submitted a proposal for *Regulations on priority on the mobile network*, suggesting that some 10,000 predefined individuals that perform critical functions in society

[35] Official Norwegian Report (NOU) 2012:14, Report of the 22 July Commission, p. 168

ought to be ensured priority to voice-based communications. The proposal does not address how members of the public can get priority, nor data communication, i.e. communication of digital emergency messages.[36] Ensuring the public priority on the network is challenging.

However, a future 112 application could be designed so that different types of data are given different priority. For example, the application could ensure that only essential and "light" information, such as phone number, location and a short text about the incident is sent if the application detects low capacity on the network. The application could then send data that requires more bandwidth, such as photos and video, when there is sufficient capacity on the network.

In the longer terms it may be pertinent to place digital emergency messages on an equal footing with voice-based emergency calls. However, this does not have to be in place before the police can start making use of digital emergency messages.

Parallel to the introduction of digital emergency messages, and while lessons are still being learnt, the police can take the initiative to find solutions that allow digital emergency text messages to have the same priority as voice-based emergency calls.

3.4.3 MANIPULATED INFORMATION

Digital emergency messages are well suited for automated processing, but are also vulnerable to manipulation and counterfeiting. For example, digital images can easily be manipulated, touched up and altered. There are many different smartphone applications that allow users to manipulate photographs. Thus there is also a risk that the information submitted by citizens may be incorrect.

This is not a new problem; even using the current systems people can report incorrect information. This problem could be overcome by legislation regulating digital manipulation of information submitted to the police, at the same time as software can be used to check whether a submitted photograph has been manipulated or not.

[36] Proposed regulations on priority on mobile networks, Norwegian Post and Telecommunications Authority 2013, http://www.npt.no/aktuelt/nyheter/_attachment/6481?_ts=13d3fec825e

3.5 INFORMATION MANAGEMENT REQUIREMENTS

A large flow of information from the public requires that the police handle this information properly. This applies particularly to the handling of sensitive personal data and the possibilities to anonymise messages and content.

3.5.1 HANDLING OF SENSITIVE PERSONAL DATA

Digital emergency messages are private or "closed" information intended only for the police. These kinds of messages may include pictures of injured people and people who are present at the scene of an incident. Emergency messages may also contain additional information such as location, health data and contact numbers for next-of-kin.

For the public to use a digital emergency message service, they must feel confident that the police will treat personal data safely and securely. Both the sender's identity and the contents of the emergency messages must be protected from unauthorised access.

This means that it must be possible for citizens to send digital emergency messages to the police securely over the Internet and that the messages must be stored securely throughout the entire information processing.

Emergency messages must be used within the bounds of the law, both initially and subsequently, and the public must be informed clearly about how submitted information will be used.

Furthermore, emergency messages ought to be stripped of sensitive personal information if its intended use does not require such information, such as when messages are going to be aggregated to track the movements of large crowds at an event.

It should also be considered whether the public should have greater freedom to decide which information they wish to submit to the police in a digital emergency message. If the sender wants to share a tip with the police, but for various reasons does not want to reveal their location, the sender ought to have the opportunity to easily remove any information considered redundant. Self-determination and the right to decide which data are submitted may be critical factors for the public to be comfortable with sharing information with the police.

3.5.2 ANONYMISATION

The sender of an emergency message or a digital public tip may wish to remain anonymous for any number of reasons. This may be because the content of the message is perceived as a risk to their own security. People ought therefore to be allowed to send anonymous tips where the name, address and other information that reveals the sender's identity is removed. Any trace on the phone that reveals that an emergency message has been sent, such as for example an electronic confirmation of receipt from the police or entries in the phone's call log, ought also to be removed. It ought to be possible to anonymise a message with a single keystroke.

In some cases photographs submitted by citizens will include people who simply happen to find themselves at the scene when the photo is taken, but who do not know that and have not consented to the photograph being sent to the police. When the purpose of a photograph is to improve the situational awareness of the police, for example by documenting a road accident, the identity of the people who were there is not relevant. Algorithms that blur faces in photographs in emergency messages before they are sent to the police may make sharing photos with the police seem less intrusive. For example, the map service Google Street View has erased all faces on all of its photographs.

Digital emergency messages can thus be adapted to the needs, and privacy-friendly solutions can be built in from the outset.

3.6 THE INTERESTS OF PRIVACY AND TRANSPARENCY

3.6.1 HANDLING SURPLUS DATA

Digital emergency messages will be able to provide more information than today's emergency phone calls. A major advantage is that the police will be able to extract important information that the sender may not even have noticed. The police will also be able to extract information that may prove to be relevant in an entirely different case. This is called surplus information.

When someone calls the police, they tell their version of an incident. It is the caller who determines what information the police receive. By contrast, photographs, video and audio recordings can provide much more information than a phone call. In a photograph, it may be possible to identify a person in the background (assuming the picture has not been anonymised by the sender) thus linking them to both a place and time that may be relevant to another case. In an audio recording, something a person says unwittingly may link them to another crime. Video contains even more information.

New links to other cases may also be found electronically if the police merge digital emergency messages from citizens with their own registers and data sets and analyse across the various sources. The person who submitted the message does not have any control over what the police can interpret and get out of the submitted information, nor whether the police will use the information for purposes other than they had assumed.

Surplus information is not information that was obtained for a given purpose. It is therefore important to have clear rules defining how the police shall be allowed, if at all, to use surplus information gleaned from digital emergency messages. When is a matter serious enough that it legitimises the use of surplus information? In what cases should the police be allowed to compare surplus information with other information that the police possess? Digital emergency messages documenting a fire might be interesting because the person who started the fire might be among the people on the scene. But should the police be allowed to check the car registration number of a car pictured passing a traffic accident against a database of sex offenders?

These kinds of questions suggest that the police ought to use surplus information with great caution and only in special cases.

Explicit rules on deleting must also be in place that ensure that digital emergency messages submitted by members of the public are automatically deleted and cannot be collated with other information indefinitely. The existing regulatory framework for voluntarily submitted DNA material could be used as a basis for regulation of material voluntarily submitted by citizens through digital emergency messages (as opposed to material that the police have collected as evidence).

3.6.2 A NEW SURVEILLANCE REGIME?

According to section 36 of the Personal Data Act, video surveillance is "continuous or regularly repeated surveillance of persons by means of a remote-controlled or automatically operated video camera (…) which is permanently fixed". Surveillance is regarded as a serious infringement of privacy and is therefore subject to strict regulation under the law in Norway. Permission for surveillance activities requires proof that surveillance is necessary, that it only covers a limited area and that the recordings will be erased at the latest 7–30 days after they were made, among other things.[37] The public must also be notified if there are surveillance cameras in public places.

In Norway, there were only 12 police cameras in the whole country in 2013. By comparison, London alone has more than 12,000 police cameras at various locations around the city.[38] Photographs from surveillance cameras played an important role in the investigation of the bombings in London in 2005. In Boston, by contrast, most of the photographs were not from police cameras, but from citizens' smartphones and private surveillance cameras.

Handheld cameras, such as mobile phones, are not covered by this legislation. At the same time, the experience from Boston shows that "crowdsourced surveillance" can be a far more powerful surveillance tool than traditional CCTV surveillance. With a smartphone in virtually every pocket, it is highly likely that major incidents in densely populated places will be documented quite thoroughly. Wearable-technology like "Google Glass" will only reinforce this trend, meaning "crowdsourced surveillance" can easily serve as a "substitute" for more extensive police surveillance. Continuous surveillance of persons can no longer be associated with a permanently fixed camera at a particular place, when there are cameras everywhere there are people.

How can we guarantee that surveillance is justified, necessary and sufficiently limited when it is members of the public taking the pictures and no one is controlling the camera?

In addition, experience from Boston shows that extensive use of citizens' photographs and video material in the investigation immediately after an incident can be problematic:

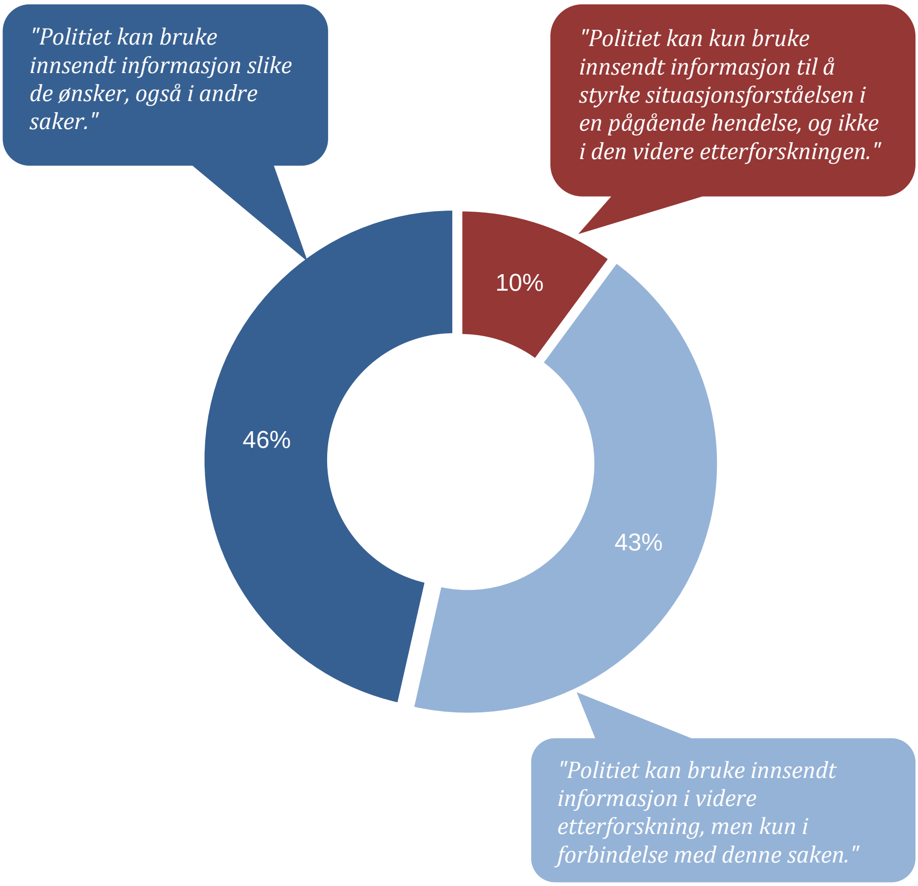
- Innocent people can more easily become mixed up in the investigation simply because they happen to be photographed "at the wrong place at the wrong time".

[37] The Norwegian Data Protection Authority (2012, version 2013): *"Camera surveillance - what is allowed?"*

[38] https://www.datatilsynet.no/Nyheter/2013/Bare-tolv-politikameraer-i-Norge/

- This may in turn result in police resources being wasted on a dead-end lead at a time when it is crucial to act quickly and make the right priorities. At the same time, it can be very unpleasant for individuals to be implicated in this way.
- In a major crisis, there is often pressure to act on the basis of information submitted by the public, before it can be adequately verified.

How should the police be allowed to use photographs and videos submitted by citizens?



"Politiet kan bruke innsendt informasjon slike de ønsker, også i andre saker."

"Politiet kan kun bruke innsendt informasjon til å styrke situasjonsforståelsen i en pågående hendelse, og ikke i den videre etterforskningen."

"Politiet kan bruke innsendt informasjon i videre etterforskning, men kun i forbindelse med denne saken."

4. THE POLICE ON SOCIAL MEDIA

Social media are a great spreader of digital information. Norwegians are among the most active users of social media in Europe.[39] In 2012, a massive 80 per cent of the population were a member of a social network.[40]

Large volumes of data are uploaded and shared on the Internet every single day. Much of this is "open" information. These data thus constitute a valuable source of fresh information. Proper analysis of real-time data from social media can quickly provide an overview of a situation. Marketing companies already use this kind of data to monitor the popularity of brands in order to be able to quickly adapt and modify their marketing campaigns.

Along with the rapid development of new tools that can analyse the information shared on these kinds of platforms, the widespread popularity of social media also opens up new opportunities for the police. Experience from other countries shows that information shared on social media can be used:

- to expose criminal activity or planned criminal acts
- to provide important intelligence tips about groups or individuals

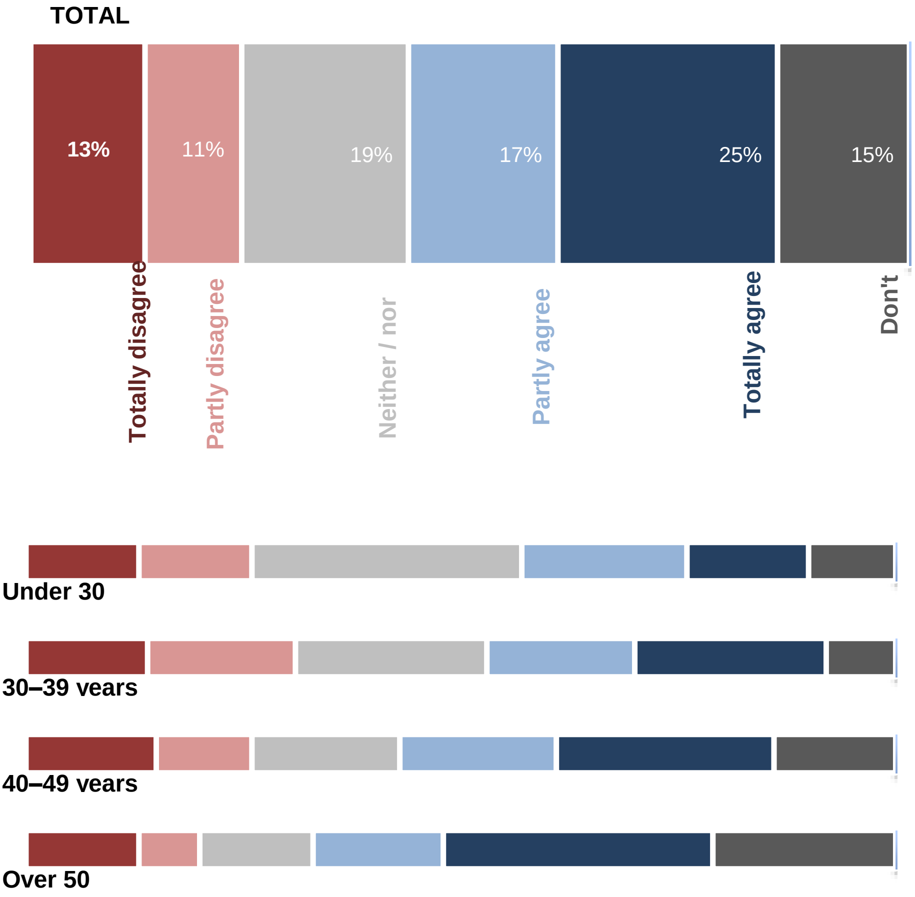
[39] http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/Information_society_statistics
[40] Facebook is by far the largest social network in Norway, with 79 per cent of women and 72 per cent of men being members. Twitter (20 per cent), LinkedIn (17 per cent) and Instagram (15 per cent) are also popular. As many as 93 per cent of Norwegians aged 15–29 have a Facebook account, while over half of people over 60 are on Facebook. TNS Gallup for the Norwegian Board of Technology and the Norwegian Data Protection Authority, January 2013

- to contribute to early warning in connection with crisis situations or major incidents
- to improve situational awareness and provide a better overview
- to engender closer collaboration with the public, based on better understanding of their perception of the police and what they are concerned about.

This chapter will address how social media can provide the police with an early warning, improved situational awareness and closer collaboration with the public.

The opportunities for both preventive and operational activities are great. At the same time, new sources of information entail new technical challenges and raise important ethical questions. Social media are a relatively new player in a rapidly growing and ever-changing digital information landscape where the old boundaries between what is considered private and what is considered public are constantly changing. Experience from the Arab Spring, and more recently the political unrest in Ukraine, has also shown that social media are becoming an increasingly important forum for public exchange of opinions. Social media have become an important arena for expression in connection with major incidents. It is therefore important that the police's use of social media does not inhibit other important roles that social media might come to play in society in the future.

I think the police ought to monitor keywords such as "demonstration", "Holmenkollen Day", "gang", etc. in open social media.



4.1 PASSIVE PRESENCE: MONITORING SOCIAL MEDIA

The Oslo Police have received much praise for their use of Twitter to increase their visibility and improve their contact with the public. However, social media may also contain useful information that the police can use to enhance their situational awareness and carry out their tasks. In this section we will look at how use of social media can:

- contribute to early warning
- provide a prompt overview of emergency situations
- identify new witnesses

We will then assess the challenges and limitations associated with this kind of information.

Like emergency messages and tips, posts on social media can contain text, photographs, video and in some cases location data. However, they differ significantly from digital tips and emergency messages in two main areas:

- information on social media is seldom targeted information intended for the police
- it can be difficult to find relevant, accurate information that can be verified

This means that social media must be treated differently to digital emergency messages. Efficient handling and interpretation of a corpus of information will be more important than quality-assuring individual posts. In this report, posts on social media are considered as value-adding supplementary information to emergency messages sent to the emergency services.

4.1.1 EARLY WARNING

A key characteristic of social media is that messages spread quickly and widely among the population, both locally and globally. During Hurricane Irene in the USA, more than 3,000 tweets were posted per minute. One minute after the earthquake in Virginia in 2011, there were 40,000 comments about it on

Twitter. Indeed, people in New York heard about the earthquake on Twitter 30 seconds before it was felt in the city.[41]

The US Geological Survey has developed an earthquake detector based on real-time information from posts on Twitter. The detector monitors tweets containing earthquake-related words and records the place, time and quantitative data. They claim that this method will enable them to issue an earthquake alert within 60 seconds of it starting. By comparison, traditional sensor-based alerts take between 2 and 20 minutes.[42] At the same time, this collection of messages forms a central catalogue of brief first impressions and photographs from people at the site of the earthquake.[43] In addition to being able to report the earthquake earlier, this system also provides an impression of the scale of the damage.

The earthquake detector is an example of how the fact that many people talk about an incident on social media can improve situational awareness and be converted into actionable information. The police could develop this kind of early warning system too, both for scheduled events that they already know about and for unforeseen incidents.

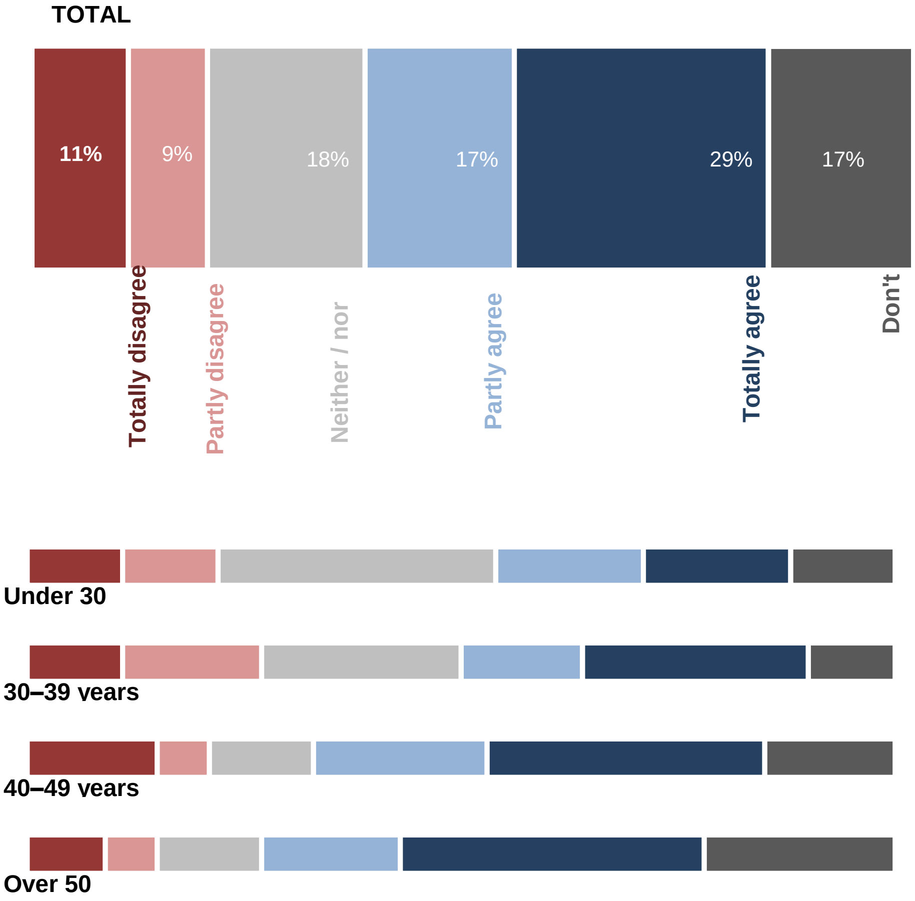
Continuous monitoring of keywords on social media could be used to signal that something significant is happening or is about to happen. Computer programs that can identify and analyse these kinds of signals on social media could be an important supplementary tool for the police to detect incidents that have occurred and that are unfolding.

[41] http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government.html

[42] http://www.livescience.com/45385-earthquake-alerts-from-twitter.html

[43] http://recovery.doi.gov/press/us-geological-survey-twitter-earthquake-detector-ted/

I think the police should track words like "shooting", "explosion" and "fighting" on open social media like Twitter in order to be able to detect incidents.



4.1.2 SITUATIONAL AWARENESS: IN SUMMARY

In crisis situations and daily incidents alike, it is important for the police to quickly gain an overall picture of what is happening. It will not necessarily be sufficient to chart the number of messages containing certain keywords – the police will also be interested in relevant content in the messages they receive.

In connection with minor incidents that generate a small amount of activity on social media, it will be a relatively simple task to extract relevant information. However, the volume of information could increase rapidly during a major incident or when there is a lot of activity on social media. Good analytical tools are thus essential for the police to be able to extract the relevant information on social media efficiently. Different analysis techniques allow extraction of relevant information from huge volumes of data, such as:

- charting the frequency of various specific words and phrases
- extracting semantic meaning from large volumes of text
- sorting and filtering messages according to various criteria
- mapping networks between various players
- reducing noise

LONDON FIRE BRIGADE MONITORS SOCIAL MEDIA

London Fire Brigade actively monitors Twitter. They search through tweets looking for keywords that match incidents that have been reported to them. For example, if a fire breaks out somewhere in London, an operator searches for the street name, neighbourhood and nearby buildings on Twitter to see if anyone in the area has tweeted about the incident. They find that this is a good way to find out what people can see and how they perceive the situation before the firefighters arrive on the scene.[44]

4.1.3 IDENTIFYING NEW WITNESSES

Analytical tools can also identify the main posters about an incident on social media. This may be the people who have posted the most about an incident or the people whose posts have been shared the most times. Both factors indicate that these people may possess information that is relevant for the police and

[44] Conversation with a representative from London Fire Brigade.

whom it might be worth contacting for follow-up and quality control of information.

4.1.4 AN EXAMPLE: 22 JULY 2011 ON TWITTER

Twitter was used frequently during the terrorist attacks on 22 July 2011. Using the analytics tool Topsy[45], we have filtered out tweets from that day containing either the word "explosion" or the words "shooting" or "shots". Figure 2 shows the cumulative incidence of posts containing these words and that was shared on Twitter in the afternoon of 22 July 2011.

Figure 2 shows a sharp increase in the number of tweets containing the word "explosion" shortly after the explosion in the Government Quarter. There was a similar surge in tweets containing the words "shooting" / "shots" shortly after the first shots were fired on Utøya.

Opportunities afforded by computer analysis

At the same time, Figure 2 shows that tweets can be regarded as digital signals and that a semi-automated analysis of these kinds of signals could serve as an early warning system. For example, even if the police had not been alerted via other channels and had only been tracking the words "shooting" and "shots" on Twitter, they would have gained a very strong indication that a shooting was under way very shortly after the first shot was fired on Utøya.

The steep rise in lines in the graph in Figure 2 also indicates a sharp increase in the number of tweets in a very short space of time. Unusual behaviour like this may possibly indicate that a major incident is unfolding and could also serve as a warning system.

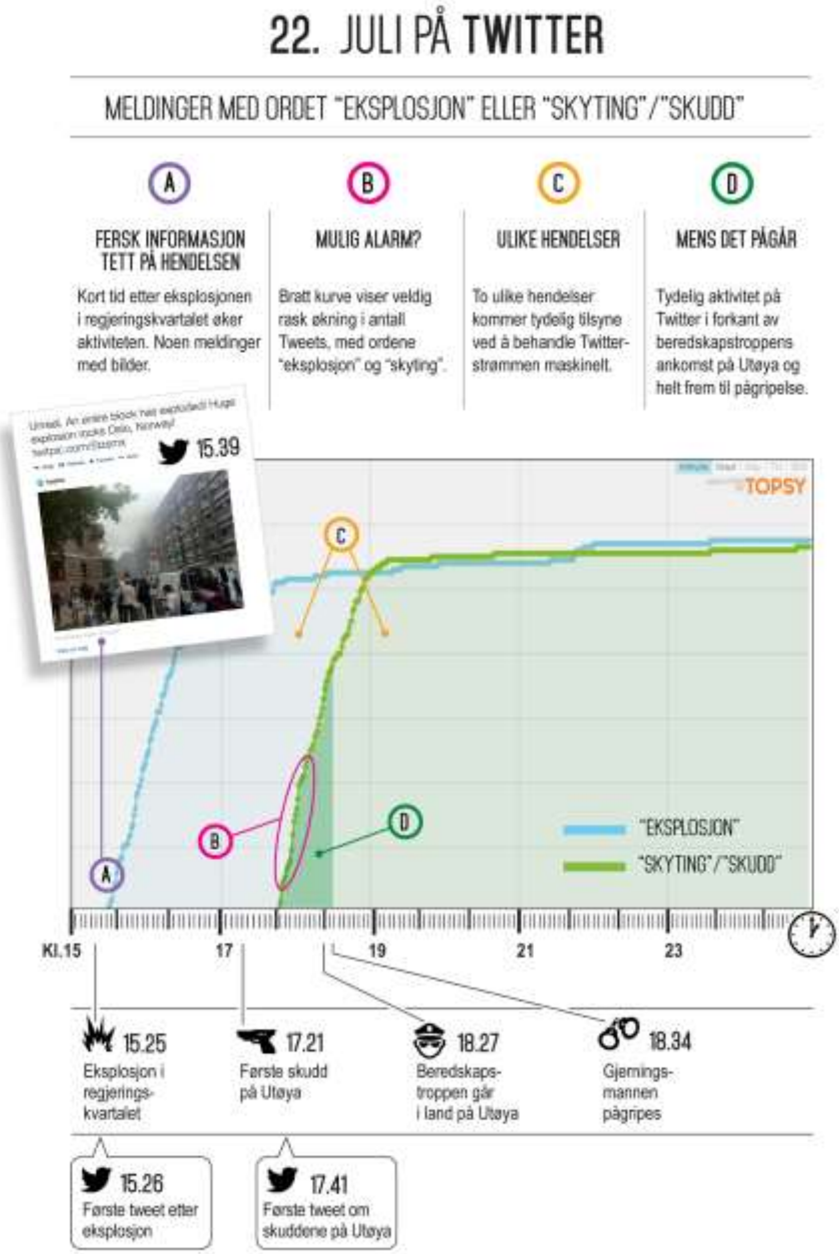
Automated analysis of social media can make it easier to handle large amounts of information and extract important and relevant information. This very simple analysis shows the two different incidents that occurred on 22 July 2011 very clearly.

Fresh information as events unfold

[45] www.topsy.com

Shortly after the explosion in the Government Quarter, there was a noticeable increase in activity on Twitter. Much of this information will probably be repetitions, but occasionally there will be posts containing information that could help improve the police's situational awareness. For example, 14 minutes after the explosion, a member of the public posted a photograph of the Government Quarter on Twitter.

Figure 2 also shows that people were active on Twitter, both immediately after the explosion in the Government Quarter and before the Emergency Response Unit arrived at Utøya and until the perpetrator was apprehended. In this way, social media provides opportunities for the police to improve their situational awareness in a chaotic situation, while an incident is unfolding.



22. JULI PÅ TWITTER

MELDINGER MED ORDET "EKSPLOSJON" ELLER "SKYTING"/"SKUDD"

(A) FERSK INFORMASJON TETT PÅ HENDELSEN

Kort tid etter eksplosjonen i regjeringskvartalet øker aktiviteten. Noen meldinger med bilder.

(B) MULIG ALARM?

Bratt kurve viser veldig rask økning i antall Tweets, med ordene "eksplosjon" og "skyting".

(C) ULIKE HENDELSER

To ulike hendelser kommer tydelig tilsyne ved å behandle Twitter-strømmen maskinelt.

(D) MENS DET PÅGÅR

Tydelig aktivitet på Twitter i forkant av beredskapstroppens ankomst på Utøya og helt frem til pågripelse.

Unreal. An entire block has exploded! Huge explosion rocks Oslo, Norway! twitpic.com/

15.39

15.25 Eksplosjon i regjeringskvartalet

17.21 Første skudd på Utøya

18.27 Beredskapstroppen går i land på Utøya

18.34 Gjemningsmannen pågripes

15.26 Første tweet etter eksplosjon

17.41 Første tweet om skuddene på Utøya

Figure 2 Tweets from 22 July 2011, analysed using the analytics tool TOPSY (Graphics by Birigitte Blandhoel).

4.2 ACTIVE PRESENCE: COMMUNICATION WITH THE PUBLIC

4.2.1 CORRECTING INFORMATION

The police and emergency services in Norway are already active on social media. They use social media to inform the public about incidents and mugging hotspots, issue tips and warnings, correct rumours and misinformation, and provide general information about the inner workings of the police. The Operations Control Room in Oslo has a Twitter account with the user name "@oslopolitiops", which has more than 131,000 followers[46] and is among the five most followed Twitter accounts in Norway.[47] The Norwegian National Mobile Police Service's Facebook page "Utrykningspolitiet" has nearly 63,000 likes.[48]

The Operations Control Room on Twitter

The Operations Control Room, which goes under the name @oslopolitiops on Twitter, won the "Best Tweet of the Year" award for the following tweet: **"Storo: We were informed about an ongoing disturbance with screaming women. When we arrived we found a party for nurses. We'll be leaving the scene soon."** The jury stated it had "(...) chosen a winner who time and again has tweeted in a manner that provides followers with fresh insight into an organisation that is both loved and hated."[49]

This kind of active presence on social media provides the police with a good platform for rapid dissemination of accurate and up-to-date information, as well as the opportunity to correct erroneous information and rumours. Posts from the police can also easily be shared, enabling information to be spread broadly and rapidly as a supplement to the more formal information channels.

The ability to spread correct information rapidly will also indirectly affect discussions on social media, ensuring they are based on correct information to the greatest extent possible. This will increase the public's understanding of the situation and contribute to a greater sense of security. Furthermore, it

[46] https://twitter.com/oslopolitiops, August 2014
[47] Ranking according to tvitre.no/norsktoppen
[48] https://www.facebook.com/utrykningspolitiet
[49] http://www.kampanje.com/markedsforing/article6482988.ece

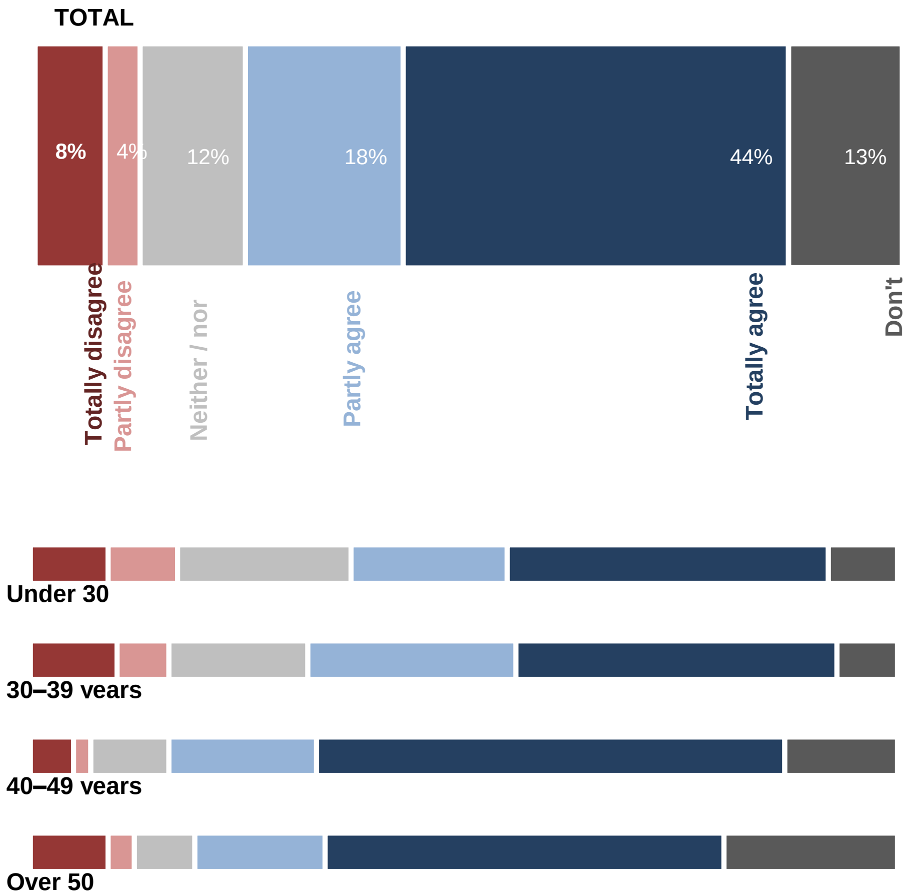
could also lead to the police receiving more accurate information from the public.

Quality control of information

In order to ensure posts from the police can easily be distinguished from other posts and to ensure their message is clear, the police and emergency services could use predefined keywords or "hashtags" in their official posts. If the police pick up on rumours and incorrect information, they could post a statement refuting the rumour and providing correct information by tagging the message with the hashtag "#AVKREFTER RYKTE: xxx" ("#REFUTING THE RUMOUR xxx").
At other times, the police may want to publish information quickly, before the contents have been verified. Then the messages could be marked with the hashtag "#UVERIFISERT: xxx" ("#UNVERIFIED: xxx").

These kinds of predefined keywords will ensure that the police's posts stand out in the flow of posts and will also ensure that they are picked up by search engines and analytical tools.

> *It's fine that the police contact me because I have posted information on social media about a serious incident.*



The police in Norway have a long tradition of working closely with the public. Good collaboration and communication with the public can be useful in a preventive context to capture early signs of developments in the local district, to receive tips in connection with a specific incident, and to better understand the causes and best solutions to problems.

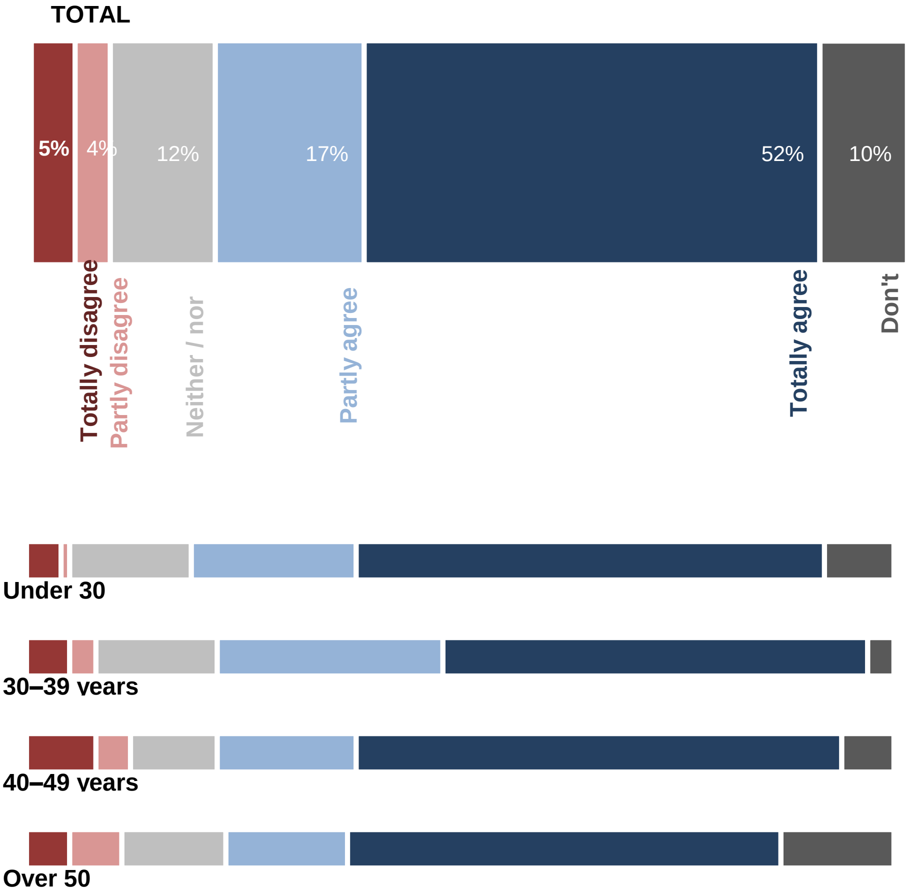
The public both want to and are willing to contribute their own experiences and collaborate openly with the police.[50] The police could expand its presence on social media to get citizens more involved, collaborate with them, and thus receive more targeted information that they can use in their ongoing work. Through active participation on these kinds of platforms, the police agencies can regularly publish public material, correct erroneous information and rumours, consult the local community and receive feedback and response. It will also enable them to remove inaccurate information, false rumours and information that infringes on other people's privacy.

The Norwegian daily newspaper Aftenposten's Oslopuls website has created a map where people can indicate places in Oslo they feel unsafe.[51] The public can zoom in on a location on the map and enter comments. Others can vote on the post, thereby indicating whether they too have a similar experience of the place. The service is moderated. These comments provide a good indication of the places that people perceive as unsafe in Oslo and constitute a good example of how the police can engage and use the public actively in their work.

[50] Iversen and Dahl (2010): *Politi 2.0: Kan sosiale medier bidra til økt dialog og samhandling mellom politi og publikum?" [Police 2.0. Can social media help increase dialogue and collaboration between the police and the public?]*

[51] http://www.aftenposten.no/nyheter/oslo/Her-foler-oslofolk-seg-utrygge-7112377.html#.UWkjYxmlgn9

The police ought to use social media as an information channel to the public, for example to issue alerts in connection with major incidents.



THE COPENHAGEN SECURITY INDEX

The City of Copenhagen has conducted a survey in which members of the public were asked about their personal experiences of crime and perceptions about crime in their local neighbourhood. The public's feedback has then been collated with the police's own data. Together they make up a so-called "security index". The security index indicates the need for measures to improve security in different parts of Copenhagen.[52] A representative from the City of Copenhagen has stated that "security in Copenhagen has improved, and the residents are less exposed to crime" since they started the mapping project.[53]

The police in several countries have used similar methods and have gained valuable experience in both monitoring and involving the public on social media. We have been inspired by initiatives from New Zealand and the United Kingdom.[54]

[52] http://subsite.kk.dk/sitecore/content/Subsites/tryghedsindeks/SubsiteFrontpage.aspx

[53] http://www.aftenposten.no/nyheter/oslo/Her-foler-oslofolk-seg-utrygge-7112377.html

[54] http://www.civildefence.govt.nz/memwebsite.nsf/Files/CDEM%20resilience%20fund/$file/Greater-Wellington-Social-media-in-an-emergency-A-best-practice-guide-2012.pdf

RIOTS IN LONDON

In autumn 2011 riots broke out in several parts of London that quickly spread across the whole of England. The following summer the London Metropolitan Police (MPS) was to be responsible for security at the Summer Olympics, the Queen's diamond jubilee and the annual Notting Hill Carnival.

MPS decided that they needed to do more to engage with the local community through social media, with a view to avoiding unrest, improving their resource planning and encouraging proactive involvement.

MPS initiated a pilot project that helped them draw up a long-term strategy for the use of social media. The pilot project showed that social media made it possible for the police to identify possible incidents much more quickly and more accurately than using traditional means. This meant the police was in a better position to implement targeted measures. They were also able to identify several potential witnesses to a stabbing. The pilot project also helped the police to build up a list of keywords that boosted the amount of available relevant information.[55]

4.2.3 PRECONDITIONS FOR GOOD DIALOGUE VIA SOCIAL MEDIA

The combination of regular publication and updating and/or correction of information to the public and continuous collection of information from the public will form a virtuous circle for efficient information processing in the police. To ensure that this kind of dialogue with the public is as efficient as possible, the police and emergency services must:

- Continuously publish up-to-date, correct and relevant information about ongoing incidents and scheduled events (both on their own website and on others' websites). By promptly publishing accurate information on many channels, the police can reduce (erroneous) speculation.

- Indicate clearly what is information from the police so that it is easy for others (both people and computers) to recognise that the message is from a government agency, while also making it easier to share.

- Monitor important keywords in order to quickly capture erroneous information and correct false rumours circulating among the public (both on their own website and on others' websites).

[55] Metropolitan Police leverage social media to engage local community with HP social media analytics tools (Case study/4AA4-5393EEW.pdf),
http://www8.hp.com/h20195/v2/GetDocument.aspx?docname=4AA4-5393EEW

- Moderate and correct erroneous information and sensitive personal data on their own websites.

- Publish information and facilitate or initiate discussions on topics and problem areas they want feedback on.

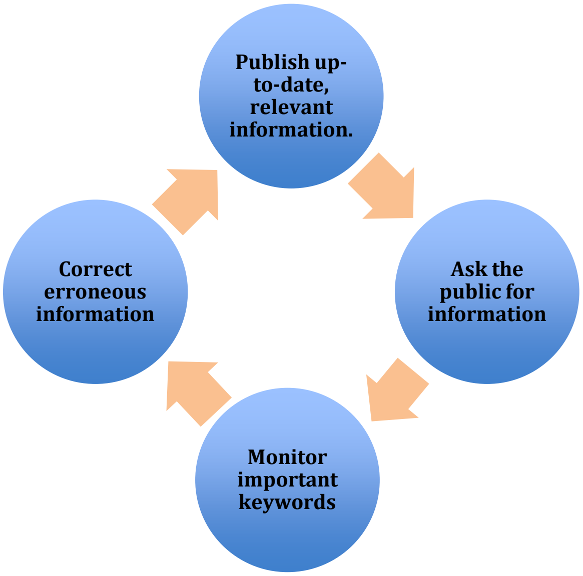

Publish up-to-date, relevant information.
Ask the public for information
Monitor important keywords
Correct erroneous information

Figure 3 Information wheel for operationalised use of social media by the police.

4.3 CHALLENGES AND LIMITATIONS

4.3.1 CAN THE POLICE RELY ON SOCIAL MEDIA?

Using information from social media can also pose challenges for the police. The information may be – deliberately or accidentally – incorrect, misleading or imprecise. Sometimes people can jump to false conclusions, and erroneous information can spread quickly.

The police have high requirements regarding verification and quality assurance of the information they receive from citizens. Information obtained from the public can be cross-checked with other information. Eyewitnesses are often called to verify details.

Posts on social media are not written with the police in mind. In many cases the police will have to interpret this kind of data to extract relevant information. This of course also entails a greater possibility of misunderstandings and misinterpretations.

This presents challenges for the police in several areas:

- how can and should the police quality-assure information from social media for their own use, without losing the real-time value of this information?
- what can and should the police do to ensure that the public as far as possible receives the right information quickly enough?

4.3.2 VERIFICATION AND QUALITY ASSURANCE

It will be both difficult and time-consuming to manually verify information from social media to the quality standards normally required by the police, especially during major crises where a vast amount of information must be handled in a very short time. The strength of social media lies in their large volumes of material. Not every post will be as useful or possible to verify in the same way as digital tips and emergency messages. However, analytical software can help.

The very fact that there are many posts describing the same situation probably indicates that the incident is real. Analytical tools can also help both verify whether an incident has occurred and assure the quality of the information.

In situations where the police receive large numbers of digital emergency messages and emergency calls, analysis of social media posts could be used to supplement, verify and quality assure the situational awareness.

Quality assurance of information can also be done by the public. Social media can function as an arena to detect and correct erroneous information from the police and emergency services. The Operations Control Room in Gudbrandsdalen reports that they use Twitter to "quality assure information from the police."[56] The police can also use the public to verify allegations: Questions such as "Has there been a landslide on national highway Rv 88?" or "Did anyone hear a loud bang in Nordberggata?" can easily be answered by social media users with a simple "yes" or "no".

4.4 PRIVACY AND TRANSPARENCY

A number of fundamental questions arise concerning the underlying principles of the police's use of social media. Social media provide the police with new information that can help improve their understanding of the situation, as well as a new platform for communication and collaboration with the public. These opportunities must be weighed up against important issues related to data privacy and transparency.

4.4.1 EXPOSURE AND PREJUDGEMENT

Immediately after the explosions at the Boston Marathon in 2013, the Boston Police Department, the FBI and several social media websites asked people to send in photographs and other material for use in the investigation. Although the police tried to channel the responses into their own dedicated channels (a phone number and e-mail address), the public also became engaged on open, social media. Eventually, a separate investigation evolved, fuelled by discussions among citizens. On the open discussion forum Reddit, a student was erroneously identified as a suspect. Photographs of this individual and other personal information were immediately published and circulated widely. Photographs were even published on the front page of the New York Post.[57]

The Boston Marathon case illustrates that smartphones and social media enable citizens to support the police's work by providing valuable data. It also shows, however, that citizens can quickly become overzealous. Once citizens become very engaged in a case, it is easy for them to initiate their own parallel investigation, thanks to modern communication tools and the rapid dissemination of information on social media. This can have very unfortunate consequences, as was the case in Boston where the public drew erroneous conclusions that were spread rapidly. This can also impede the police's work. It is

[56] http://www.fjuken.no/index.cfm?event=doLink&famID=318350&frontFamID=84050
[57] http://www.bbc.co.uk/news/technology-22214511

therefore necessary to have clear mechanisms that allow citizens to contribute information, but not take part in the investigation.

4.2.2 SENSITIVE PERSONAL DATA

Witness observations may contain sensitive personal information and may violate other people's privacy. This type of information is not suitable for open discussions. Certain types of information will not be suitable for open sharing in public forums for tactical reasons.

However, the police are not responsible for and do not have control over what is communicated openly on social media. In theory, everyone has the right to say what they want on social media, as long as they abide by the general statutory provisions on freedom of expression defined in Article 100 of the Constitution. Nevertheless, the experiences from Boston prove the need for a clear strategy on the use of social media by the police.

In the mean time, the police can reduce the risk of sensitive personal data being spread by:

- moderating discussions on their own social media channels
- directing sensitive personal data to the closed channels into the police such as telephone, SMS, MMS and digital tips and emergency messages.

4.4.3 WILL THERE BE A CHILLING EFFECT?

We want an open society with freedom of expression, without everything we say on social media being archived and analysed by the state with the possibility of it being used against us on a later occasion. At the same time we want the police to have the best chances to be able to perform their tasks in the best possible way. The question is: if we know that the police are monitoring social media, will we express ourselves differently or use these services differently?

The "chilling effect" refers to the phenomenon whereby people refrain from using a service or in some way moderate or limit their use out of fear for how the information might be used. This kind of chilling effect may result from both conscious and unconscious choices we make.

In a survey that the Norwegian Board of Technology conducted in collaboration with the Norwegian Data Protection Authority, 1 out of every 4 Norwegians stated that they have refrained from signing a petition because they are unsure about how the information can be used later. 1 in 10 have unsubscribed from a social website for the same reason.[58] In the Norwegian Board of Technology's survey conducted in conjunction with this report, almost 2 out of 5 respondents stated that they would avoid using words and phrases that are monitored by the police.

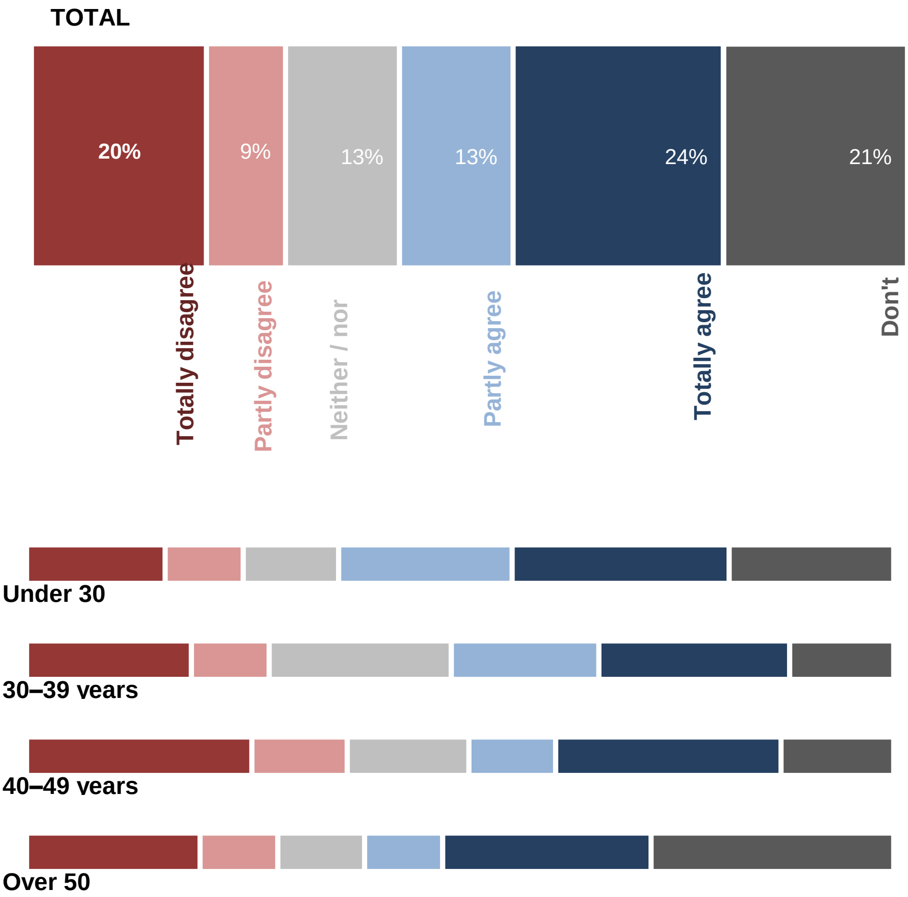
Although a certain degree of self-censorship is a natural aspect of most people's every-day digital life, it is important that the authorities' use of digital information does not lead to a development that undermines freedom of expression in an open democracy. In many places social media have proved to be an important arena for discussions and political participation.[59] Both during the "Arab Spring" in the Middle East and North Africa in 2011 and during the political turmoil in Ukraine in 2014, social media were important instruments in the public exchange of opinions.

Lack of transparency and clarity in routines and guidelines for the use of information on social media can have a chilling effect on freedom of expression. The same can also happen if the police monitor information from social media, even if it is an open forum.

[58] Personvern 2014 – tilstand og trender [Data privacy 2014 – status and trends], the Norwegian Board of Technology and the Norwegian Data Protection Authority, January 2013

[59] Social Media and Human Rights, Commissioner for Human Rights, Council of Europe, February 2012,

If I knew that the police were monitoring specific words and phrases on social media, I would avoid using those words.



4.4.4 HOW "OPEN" IS INFORMATION POSTED ON SOCIAL MEDIA?

Our attitudes to what is regarded as private and what is regarded as public are constantly changing. On social media it can be particularly difficult to distinguish between private and public information. How do we decide what is the public domain, what is private space and what is possibly a new hybrid between public and private? There are many different social media, which all operate in different ways. Some are completely open, some require registration and log-in to view the content, while others operate with a variety of forums, of which some are more open and others are more closed. Facebook is a major social networking community that requires log-in. Some parts of the exchange of information and opinions are open to all members, while other parts take place in more closed forums.

Whether information on social media is shared broadly or not is determined partly by the service and partly through conscious choices that the user makes through settings offered by the service. However, as these settings become more complex and the default settings are geared towards active, broad sharing, it is unreasonable to assume that all users at all times are fully aware of how much and how broadly information they post is actually being shared.

- Technical openness is thus not always synonymous with intentional openness.

Nevertheless, the police ought to be able to use any information that is openly available to all other players in society. Tweets can be read by anyone with Internet access and must therefore be regarded as open information. Tweets thus have clear parallels to information in the mass media. However, it is less clear whether information that is shared openly with, for example, all logged-in Facebook users should be regarded as open or closed information. This information may be unavailable to a normal Internet search engine, yet openly available to many thousands or even millions of logged-in users.

- In other words, just because information is technically "closed" and only available to a limited audience does not mean that it has not been shared very widely and with very many people.

It might be natural to define information as open if it is available through a normal search engine, but even this kind of definition will necessarily be volatile and somewhat arbitrary (shall Google's indexing and search algorithms determine what is open information and what is closed?), because these tools are constantly evolving. A technical definition of the distinction between private and public on social media will therefore always struggle to capture all the nuances of what people perceive as public and private information. Nevertheless, broad availability among the general public and other social players could be used as a criterion to qualify information as open.

By contrast, information that is shared in closed forums and that is intended for a limited group of people only cannot as obviously be regarded as open information. To gain access to this kind of information, typically not only log-in with the service is required, but also membership in a particular group or "friendship" with a particular user. Even if the police openly and transparently apply for membership of the group in question, data collection will be taking place in a closed "private space" and will therefore have parallels to undercover surveillance operations.

It will be a challenge to draw clear distinctions between what people regard as public and what they regard as private on social media. This has not been properly clarified in Norway, as was clearly demonstrated in the Nettby case.

NETTBY – ARE OLD ONLINE UTTERANCES PUBLIC INFORMATION?

"Nettby" was established in 2006 and from 2007 to 2009 was Norway's largest social networking community. The service was available to everyone, but required registration and log-in to use. Like Facebook, Nettby operated with both open and closed forums. Some information was made available to everyone; users could limit other people's access to other information. The service was discontinued in 2010.

After it was closed the Norwegian Data Protection Authority demanded that all data relating to the website be deleted. According to the Norwegian Data Protection Authority, utterances made on the website were to be regarded as private because the service required log-in. By contrast, the owner of the service, VG, held that some of the utterances should be regarded as public information, in part because they were available for indexing in general search engines and thus available to everyone on the Internet. (The Privacy Appeals Board dismissed VG's appeal, and VG had to delete all the material from the Nettby website).[60]

As other sectors start using information from social media to a greater extent, it is only natural that the public will expect that the police are even more sophisticated in their use of these kinds of tools. At the same time the police's

[60] http://www.personvernnemnda.no/vedtak/2012_03.htm

use of social media must have both wide acceptance and the consent of the citizens. This requires clear understanding of what is considered acceptable practice and what is perceived as intrusive behaviour. Activities must be firmly rooted in relation to these distinctions.

4.4.5 OPENNESS AND TRANSPARENCY REQUIREMENTS

Openness about the purpose of surveillance, what the received information will be used for, what kind of keywords are being monitored, and how long the information will be stored for will be essential to gain the necessary trust of the public. The police can overcome this issue by, for example, publishing information on:

- **Purpose**
  The purpose of monitoring social media and what the information will be used for. For example, one possible limitation might be that information is only used to improve the general situational awareness and is not used to identify individuals or as part of an investigation.
- **Sources and methods**
  Which social media are being monitored, and details about when this is done and the methods used to collect and analyse data.
- **Keywords**
  Openness about which generic keywords are continuously being monitored ("shooting", "bomb", etc.).
  In connection with specific events (such as a state visit, sports event or scheduled demonstration), the police ought to explain the correlation between the specific event and the type of keywords being monitored.[61]
- **Storage time**
  How long search results are kept for ought to be proportionate to the purpose of the monitoring. For example, information received in connection with a rescue operation can be deleted shortly after the rescue operation is completed.

The police and emergency services that use information from social media ought also to be subject to supervision to check that they only monitor the keywords that they have announced they will be monitoring.

[61] In terms of the monitoring of keywords related to specific events, the keywords will often vary depending on the nature of the event. There may be good reasons for the actual keywords being monitored not being shared with the public.

4.4.6 GUIDELINES FOR THE POLICE ON SOCIAL MEDIA

Communication between the police and the public is the backbone of a modern police force. Social media are an important means of sharing information in society today. Although there are challenges associated with the police being on social media, the potential rewards are so great that the police ought to start considering now what arrangements they need to make to be able to use information from social media on a larger scale.

GUIDELINES FROM THE LONDON FIRE BRIGADE

The London Fire Brigade is one example of how guidelines for use of data from social media can be designed. They have developed what they call "house rules", which describe the ground rules for discussions on their Facebook page. They want a friendly, polite tone and will not tolerate bullying or harassment, by other users or by Fire Brigade employees. They would prefer not to exclude people or remove content, but will do so in cases they regard as serious enough.[62]

The current guidelines for how the police shall behave on social media largely deal with how the police should convey information to the public. Citizens can post a message on social media that is intended for the police, but the police are not obliged to read posts or respond to them. However, the police do respond to and moderate citizens' posts on their Facebook pages or their Twitter accounts to a certain extent.[63]

One of the keys to the success of the data collection after the Boston Marathon bombings was that the police already had guidelines in place. The police therefore knew how to use social media to handle the situation.[64]

The police and emergency services in Norway have a good platform to build on to reverse the flow of information and start gathering information from social media. Clear and transparent guidelines will be important and necessary to achieve a good dialogue with the citizens. The guidelines will also be able to justify the removal of information and as applicable the exclusion of users who repeatedly post inappropriate messages. This will help build trust in and legit-

[62] https://www.facebook.com/LondonFireBrigade/app_128953167177144

[63] http://politiforum.07.no/id/3879

[64] http://www.london.gov.uk/sites/default/files/Police%20technology%20report%20-%20Final%20version.pdf

imacy for the police's presence on social media. At the same time, the police can initiate pilot projects to gain experience in using social media in a police context. These two processes ought to run in parallel and provide one another with mutual input and inspiration. The guidelines should answer the following questions and be openly shared with the public:

- Which social media are being monitored and for what purpose?

- The methods used in this monitoring, and an assessment of whether the relationship between the purpose and the methods is proportional and necessary.

- How long the collected information will be archived for and how the information can be used and collated with other information.

- The purpose of an active and open social media presence. The type of communication that the police hope to achieve with the public and what is unacceptable practice.

- What mechanisms the police will use to protect people's privacy when citizens are actively involved in a case or an issue on social media.

When the Police Register Act comes into force on 1 July 2014, these guidelines ought to be taken into account in the application of the regulations.

5. REFERENCES

DOCUMENTS FROM NATIONAL AUTHORITIES

The Norwegian Data Protection Authority (2012, revised 2013): *Kameraovervåking – hva er lov? [Camera surveillance – what is allowed?]*

The Norwegian Data Protection Authority and the Norwegian Board of Technology (2014): *Personvern 2014 – tilstand og trender [Data privacy 2014 – status and trends]*

The Directorate for Civil Protection and Emergency Planning (DSB) (2013): *Digital kommunikasjon med nødstilte [Digital communication with people in emergency situations]*

Recommendation no. 425 to the Storting (2012–2013): *Recommendation from the Standing Committee on Justice concerning preparedness for terrorism. Follow-up of Official Norwegian Report (NOU) 2012:14, Report of the 22 July Commission. Recommendation to the Storting from the Standing Committee on Justice, Oslo.*

Iversen, T and Dahl, I. 2010. *Politi 2.0: Kan sosiale medier bidra til økt dialog og samhandling mellom politi og publikum?" [Police 2.0. Can social media help increase dialogue and collaboration between the police and the public?]*

Report no. 21 to the Storting (2012–2013): *Preparedness for terrorism: follow-up of Official Norwegian Report (NOU) 2012:14 Report of the 22 July Commission*. Report to the Storting (white paper), Oslo.

Official Norwegian Report (NOU) 2012:4 (2012): *Report of the 22 July Commission*. Official Norwegian Report, Oslo.

Official Norwegian Report (NOU) 2013:9 (2013): *Ett politi - rustet til å møte fremtidens utfordringer. Politianalysen. [One police – equipped to meet future challenges (The Police Analysis)]* Official Norwegian Report, Oslo.

PUBLICATIONS

Omand, D., Bartlett, J., Miller, C. (2012): *#Intelligence*

Queensland Police Service (2011): *Disaster management and social media – a case study*. Queensland, Australia.

Rive, G., Hare, J., Thomas, J. & Nankivell, K. (2012): *Social Media in an Emergency: A Best Practice Guide*. Wellington Region CDEM Group, Wellington, New Zealand.

London Assembly (2013): *Smart Policing. How the Metropolitan Police Service can make better use of technology*. Budget and Performance Committee. London, United Kingdom.

Government 2.0 taskforce (2009–2010): *Social Media helping Emergency Management – Final Report*. NGIS Australia, Australia.

United Nations Global Pulse (2013): *Mobile Phone Network Data for Development*

CITED WEBSITES

Earthquake map of Haiti: http://irevolution.net/2012/02/26/mobile-technologies-crisis-mapping-disaster-response/

Earthquake detector: http://recovery.doi.gov/press/us-geological-survey-twitter-earthquake-detector-ted/

The police and Twitter:
http://www.kampanje.com/markedsforing/article6482988.ece

Trygghetskart [The Security Map]:
http://www.aftenposten.no/nyheter/oslo/Her-foler-oslofolk-seg-utrygge-7112377.html#.UWkjYxmlgn9

Danish Security Index:
http://subsite.kk.dk/sitecore/content/Subsites/tryghedsindeks/SubsiteFrontpage.aspx

The British police's pilot project:
http://www8.hp.com/h20195/v2/GetDocument.aspx?docname=4AA4-5393EEW

The Privacy Appeals Board's decision in the Nettby case:
http://www.personvernnemnda.no/vedtak/2012_03.htm

Guidelines from the London Fire Brigade
https://www.facebook.com/LondonFireBrigade/app_128953167177144

The Oslo Police's Twitter account: https://twitter.com/oslopolitiops, August 2014