Tracking in Public Spaces

The use of WiFi, Bluetooth, beacons and intelligent video analytics.

Juni 2016

Datatilsynet
The Norwegian Data Protection Authority

Contents

Introduction – From online tracking to tracking in the physical world

Looking at which sites a person visits online provides useful information for a range of companies and businesses. Facebook, Google, and Microsoft, along with thousands of companies in the advertising industry, are dependent upon knowing and understanding their users, and they use a range of technologies to monitor individuals' online activity.

The best-known of these technologies are *cookies*, *always logged in* (the fact that a user remains logged in until they actively log out), and *device fingerprints*. It is possible for a user to be tracked across devices. Even if we log out of our computers, we remain online through our mobile phones.

For a long time, only our online activity was registered. This has changed due to the proliferation of smarter phones and other devices that we carry with us constantly. Mobile phones has thus made it possible to track us in the physical world as well.

In recent years, Norwegian companies and businesses have developed an increased interest in tracking our physical movements. Some companies use tracking technologies to calculate traffic delays during rush hour traffic or to estimate the waiting time at airport security. Others want to map and analyse their customers' movements through shops and shopping centres in detail. Overall, the companies utilising tracking technologies are very different and pursue a wide range of objectives.

The theme of this report is tracking technologies used in public spaces. By 'public spaces' we refer to places that are open to the public, such as shopping centres, shops, streets, public transport stations and stops, and entertainment venues. We are concerned with tracking technologies because tracking and surveillance of individuals' movements and behaviour can violate the right to privacy and data protection. This is especially the case if individuals are tracked covertly or in an invasive manner.

Google and tracking

Google was the first company to start gathering detailed information on our physical movements on a large scale. The Google Maps mobile app can trace the user's precise location using GSM base stations, GPS satellites, and similar tools.

In 2008, Google's Street View vehicles began to map the locations of WiFi networks. As a result, a user's location can be identified by which WiFi network they are connected to. This has provided Google with knowledge on their users' movements.

Scope and outline

This report examines four different technologies that can be used to track individuals: WiFi, Bluetooth, beacons, and intelligent video analytics (IVA). Technologies such as GSM, GPS and IP tracking, RFID, and audio tracking will not be examined in detail, but some of them will be referenced to on occasion to illustrate the potential uses of tracking technology.

The outline of the report is as follows: firstly, the report will describe the tracking technology – how it works and how widespread it is. Secondly, we will examine the privacy implications of the technology. Finally, we will introduce guidelines for businesses, companies and agencies on how they can use tracking technology legally and in a manner that does not infringe upon individuals' right to privacy.

WiFi and Bluetooth tracking

WiFi

WiFi is a wireless technology that enables electronic devices, such as mobile phones, to connect to the internet. Areas where WiFi is used are typically referred to as wireless networks or WiFi zones. Today, WiFi zones are found everywhere, from private homes to workplaces, trains, cafes, shops, aeroplanes, and petrol stations. WiFi is popular because it tends to be a cheaper and faster way to surf the net than using mobile data.

When WiFi is activated on a mobile device, the device will continuously search for WiFi zones nearby. A WiFi zone can have a range of 50 to 100 metres from the WiFi access point. When searching, the device emits a unique signal called a MAC address. If an area contains multiple WiFi access points, a phone's MAC address can be registered by all of them. This information can indicate how long the user has been in that location as well as the direction in which they are moving.

Mac address

A MAC address is a unique ID number that can identify your mobile device. It is issued by the manufacturer. A MAC address is defined as personal data when it is collected through WiFi tracking.

WiFi tracking entails registering and saving the MAC addresses emitted by mobile devices for purposes other than giving that device access to a WiFi network. Since most people today own and use a mobile phone, the number of MAC addresses within a given area will give a fairly precise picture of how many people are present at that location as well as their movement patterns. In this way, the owner of the WiFi network can collect data on the position of mobile users (positional data) within the WiFi zone.

The companies and businesses that utilise WiFi tracking are interested in positional data. They are looking to collect information about *where* the owners of mobile devices are, in order to count, analyse, and compare information on users' movements for various purposes.

A MAC address can thus be traced to a particular person, because it is unique to that person's telephone or device. This person can be identified both directly and indirectly in several ways – for example, mobile operators and providers can keep records of phones' MAC addresses.

Furthermore, users are often required to provide directly identifying information, such as an email address, to gain access to public WiFi networks, and this information can be paired with their device's MAC address. A person can also be identified indirectly through positional data, habits, and movement patterns revealed by the WiFi tracking. For these reasons, MAC addresses constitute personal data.

WiFi tracking cannot take place if WiFi is completely disabled on a mobile device. Users should be aware that certain WiFi functions remain active on certain devices even when WiFi appears to be deactivated. To ensure that WiFi is completely disabled, it may be necessary to review the device's advanced settings.

Bluetooth

Bluetooth is a wireless technology that is used to transfer data between electronic devices, e.g. between a mobile phone and a PC. Bluetooth shares many similarities with WiFi, but uses less power and has a shorter range.

When Bluetooth is activated on a mobile device, the device sends out a unique signal called a Bluetooth MAC address. Bluetooth tracking entails registering and saving the Bluetooth MAC addresses emitted by mobile devices. This is used to track the users' movements.

The advantage of using Bluetooth for tracking rather than WiFi, is that Bluetooth technology can provide more accurate information on the user's location within a limited area, due to the shorter range.

Bluetooth tracking can be avoided by deactivating Bluetooth on the phone or device. Be aware that Bluetooth may be activated automatically on certain mobiles following software updates or when the phone is restarted. On certain devices it can be difficult, and in some cases impossible, to deactivate Bluetooth in a simple manner, such as in cars.

Prevalence and usage

There is considerable interest in WiFi tracking, and this technology is in use throughout Norway. As WiFi tracking comes in several different forms, it is difficult to draw firm conclusions about its prevalence and distribution.

There are WiFi solutions that enables the counting of people over time. In addition, some solutions make it possible to link a MAC address to directly identifying information. For example, some WiFi networks have a feature that allows the network to extract information from Facebook about a user when they use the network to log into Facebook. A store can use this information to check on its customers' interests.

WiFi tracking

If you submit your name or email address when you connect to a WiFi zone, the owner of the network will be able to connect your device's MAC address to your identity. This makes it possible to follow your movements within the WiFi zone through the signals that are constantly emitted from your device. If the WiFi point is in a sports store, the owner of the network knows both that you have been in the store and the exact time at which you visited.

Many guest networks at conference centres and hotels can also save MAC addresses in order for recognized devices to be logged in automatically, but this is not done to track individuals. The Norwegian Data Protection Authority has no reason to believe that WiFi tracking is widespread in shopping venues, but we are aware that many shopping centres have begun to look into such technologies.

A prominent example of the use of WiFi tracking can be found in airport security at Oslo Airport, Gardermoen. The airport uses WiFi tracking to estimate the waiting time to pass through security. The tracking is carried out by positioning a number of WiFi access points before and after the security desks. The times at which individuals pass each of these points are combined to calculate how long it has taken to move between them, giving a fairly precise indication of the average transit time through security. This information is conveyed to other travellers on regularly updated information screens.

Another example of WiFi tracking in Norway can be found at the *CC Stadion* shopping centre in Hamar. The centre uses technology that has the potential to map and analyse the movements of its customers, which again can be used to provide targeted advertising and optimise product positioning. The centre's management says[1] that it will always obtain customers' consent before using this technology to analyse individuals' movements and provide targeted advertising. Without such consent, the centre will only count the number of visitors.

There have been several privacy cases regarding WiFi tracking in other European countries. In Sweden, the Swedish Data Protection Authority carried out an investigation into WiFi tracking in 2015[2]. WiFi tracking was used in a city to map people's movements around the city centre. The purpose was to collect MAC addresses to compile statistics on the number of visitors to the city core. The Swedish Data Protection Authority determined that the WiFi tracking in question was unlawful, since it made it possible to monitor individual's movements in a public space. The company responsible for the tracking was ordered to either amend or cease the practice. The company implemented changes so that MAC addresses were deleted almost immediately, with the result that statistical data could no longer be traced back to individual phone owners. In addition, information boards were posted in the town centre, and information was published on the company's website. The Swedish Data Protection Authority found these changes to be sufficient and accepted the WiFi tracking as it was then carried out.[3]

In the Netherlands, the Dutch Data Protection Authority carried out an investigation in 2015 into a company

[1] Hamar Arbeiderblad (08.11.2014): http://www.h-a.no/nyheter/overvaaker-kundenes-bevegelser

[2] Datainspektionen.se (23.6.2015): http://www.datainspektionen.se/press/nyheter/2015/besoksflodena-i-vasteras-mats-for-noggrant-/

[3] Datainspektionen.se (02.11.2015): http://www.datainspektionen.se/press/nyheter/2015/gront-ljus-for-besoksmatning-i-vasteras/

producing WiFi solutions for tracking in stores[4]. The tracking system was used to monitor customers' movements within the stores by registering the MAC addresses of their phones. The MAC addresses of the phones of passers-by in the streets outside of the stores were also registered. The purpose was to analyse customers' movements and shopping patterns, and the data was stored for an unlimited period. Neither the customers nor the passers-by received any information that the signals from their devices were being registered and stored. The Dutch Data Protection Authority found the practice unlawful on the grounds of insufficient information as well as failure to anonymise and delete MAC addresses.

Privacy implications

WiFi and Bluetooth tracking technologies use our own devices to track us – devices for which voluntary communication is the original intended purpose. By way of WiFi and Bluetooth tracking, our devices can be used for new purposes without our knowledge. Surveillance of our movements for counting, mapping, and analysis can be uncomfortable and offensive, especially if we are unaware of who is monitoring and for which purposes.

In the real world, the companies and businesses who are tracking us are far less visible than the little goat in Alf Prøysen's famous fairy-tale (see the box below). It is difficult, and often impossible, to know if our phones' WiFi and Bluetooth signals are being tracked. In the Swedish and Dutch cases outlined above, WiFi tracking in public spaces was taking place in secrecy until the authorities took action. Covert tracking has privacy implications as we lose control over our own personal data and are no longer able to exercise our right to make informed choices or exert influence.

When certain companies or businesses know a great deal about us, while we know nothing about them, their power is increased. This can generate advantages for those who know the most – an advantage that companies and businesses can use to influence us or to make decisions with practical consequences to us. One example could be the price of an individual item differing from customer to customer based on an analysis of how much each customer would be willing to pay. The uneven playing field leads to information asymmetry, which constitutes a form of market failure. When the consumer does not possess knowledge of what is happening, they are unable to demand more privacy friendly services. The uneven distribution of information results in a form of competition that encourages companies to use increasingly privacy-invasive tools.

A fundamental principle of privacy is that the collection of personal data should not take place covertly. This is why the Personal Data Act requires companies to give information whenever WiFi or Bluetooth tracking is taking place.

The little goat that could count to ten

Alf Prøysen's story of the little goat that could count to ten illustrates the discomfort that can arise due to lack of information. Once upon a time, the story begins, there was a little goat that had learnt to count to ten. He began to count the other animals, without explaining what counting was or why he was doing it. This made the other animals afraid and upset. They decided to "get" the little goat and teach him a lesson. Fortunately, the story ends well as the goat saved all the other animals from drowning when his counting abilities proved useful on a boat that could only hold ten passengers.

The story illustrates the importance of transparency and understanding why something is happening. In the story there was no big company counting the animals – just a little goat. Nonetheless, it still made the larger animals angry and afraid because he counted them without telling them what he was doing and why.

[4] Autoriteit Persoonsgegevens (1.12.2015): https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/conclusions_bluetrace_investigation.pdf

Information gives us the power to protect our rights and ensures transparency. Transparency contributes to the legitimate and fair use of personal data. Everyone who is subject to tracking has, for example, the right to access the personal data concerning themselves that is being processed.

Pursuant to the Personal Data Act, tracking requires consent. The ability to refuse to give consent gives us freedom of choice and control over our own personal data. Sometimes, however, simple counting can take place if it is necessary to protect a legitimate interest that outweighs the individual's right to privacy. Since tracking constitutes an interference in our private lives, it must be both necessary and justified. If we find the use of tracking technologies useful for public purposes, it is easier to accept it.

When MAC addresses are used to count people, it may be necessary to store the addresses for a limited period. Storage may be necessary to avoid double counting – one needs a list of the MAC addresses already counted in order not to count them again.

On the other hand, an excessive storage period can make it possible to track us over longer periods of time and across areas. When multiple WiFi access points are connected to the same network, it is possible for the network owner to see which access points a person passed by and when, enabling them to follow that person's movements. For example, a person's movements through a shopping centre could be tracked over the course of a year, or a chain of stores could track a customer every time they entered one of the stores.

It is therefore important that MAC addresses are not stored any longer than necessary. They should be deleted as soon as possible to avoid invasive and disproportionate tracking.

Sometimes the places we visit can reveal our state of health, religious beliefs, political views, or sexual orientation. This information is considered as *special categories of personal data*, and strict rules apply to the processing of such data. WiFi tracking should therefore be avoided in certain locations, such as medical clinics, places of worship, or during political demonstrations.

§ Consent

When a company handles personal data, as a main rule, the processing should be based on consent. This means that you agree to allow the company to process information about yourself.

For consent to be valid, it must be informed and freely and actively given.

Guidelines for the use of WiFi and Bluetooth tracking

1. WiFi and Bluetooth tracking can take place if valid **consent** is obtained from the persons being tracked. Brief counting may take place without consent if the measure is necessary to protect a legitimate interest that outweighs the individual's right to privacy. This entails considering whether it is possible to achieve the purpose using less invasive measures, for example by using sensors that do not collect personal data.

2. **Connecting** WiFi and Bluetooth tracking with email addresses, customer accounts, Facebook profiles, or similar information, can only take place if consent is obtained from the persons being tracked.

3. Tracking of people **over time** can only take place if consent is obtained from the persons being tracked.

4. The **purpose** of the tracking must be clearly defined. The tracking measure can only be used in line with this purpose, and personal data collected cannot be reused for other purposes later.

5. It is unlawful to collect more personal data than is **necessary and relevant** for the purpose.

6. **Avoid** using tracking technologies in locations that can reveal a person's state of health, religious beliefs, political views, or sexual orientation.

7. **Security measures** must be implemented to protect the personal data so that it does not go astray.

8. **Information** must be provided whenever tracking takes place, using signs or other clear information sources. The information must include what kind of tracking is taking place and what the purpose is – e.g. the compilation of customer statistics. It must also state who the controller (entity responsible) is and include the controller's contact information. This information must also be included in any privacy statements.

9. There must be **clear procedures** for how long MAC addresses are to be stored. MAC addresses must be deleted as quickly as possible so that it is not possible to link the information back to individuals. Meanwhile, security should be adequately maintained by pseudonymising the MAC addresses.

10. **Notification** must be given to the Norwegian Data Protection Authority.

Pseudonymisation

When MAC addresses are to be pseudonymised, this can be done with the help of hashing.

Hashing, also referred to as a cryptographic hash function, is a method of converting MAC addresses to a code consisting of numbers and letters. The same MAC address will always result in the same code, but it is impossible to trace that code back to the original MAC address.

Beacons

Beacons are small battery-powered devices that transmit information that can be picked up by nearby mobile phones. The signals are transmitted using Bluetooth technology, and the coverage area may have a radius of up to 70 metres. In theory, only an app belonging to the company that deployed the beacons can read these signals, but in practice, other applications and operating systems (such as iOS and Android) can read them too.

All beacons emit a unique ID. When an application reads the ID, it can trigger an action in the app, such as the delivery of a message or advertisement to the user. Too many messages can, however, annoy the user, so sometimes it will not be visibly apparent that a beacon has been read. The app can detect if a mobile phone enters or exits a predetermined zone, and this can be registered in the background. Whoever responsible for the app can thus identify which beacons the user has been close to, at what distance, and at what time, without the user noticing.

Example

A customer has downloaded an app from a sports store to their mobile phone. The store has deployed beacons. When the customer is in the store, the app can *see* that the customer is spending most of their time in the bicycle department. When the customer leaves the store, a message appears on their mobile with an offer of a 20% discount on bicycle gear the next time the customer visits the store.

There are various technical solutions when it comes to beacons, each with its own set of advantages and disadvantages. Beacons can be divided into three main groups:

- *iBeacons*, which is Apple's solution
- *Eddystone*, which is Google's solution
- Other proximity beacons, such as *AltBeacon (The Open and Interoperable Proximity Beacon)*

Apple states that an application can only use **iBeacons** to localise a person if the person has given prior consent. The user will also be notified by a location symbol that appears in the status bar at the top of the screen.

Google's Eddystone can send out URLs (links to websites) that can be read by the Chrome web browser. This means that it is not necessary to download a dedicated app for different beacons – all of them are compatible with Chrome. To avoid spam, all URLs from Eddystone first appear on mobiles as push messages, so that the user can choose whether to open them. Information about the user will not be registered until the link is opened. Thus, the owners of various beacons will not obtain knowledge about who is close to their beacons before the user opens the links.

AltBeacon utilises an open solution for beacons. Open solutions make it possible for a single application to manage beacons deployed by several different businesses. For example, a shopping centre's app could handle messages and localisation for the various stores located in the centre. We will therefore see apps that read beacons across multiple businesses and locations. The best-known solution for this is *Facebook Place Tips for Businesses*.

Just as with Bluetooth tracking, tracking by beacons can be prevented by turning off Bluetooth on your phone or device.

Beacons may also transmit information using other technologies, such as sound frequencies that are inaudible to humans. One such service is Google's *Nearby*. This service uses a combination of WiFi, Bluetooth and inaudible sound frequencies to connect to nearby devices.

Audio tracking does not require dedicated beacons, since audio signals can be transmitted from most electronic devices. For example, an audio signature can be played by our computer when we visit a particular website or by the TV during a commercial. These audio signals can be picked up and registered by other devices, such as mobile phones. This technology will therefore make it easier to track people across multiple devices, and between the internet and the physical world.

Prevalence and usage

Beacons have been available on the market for a while, and demand is growing. It is estimated that there are already thousands of beacons deployed in Norway alone, and this number will most likely increase. Beacons are used by, among others, entertainment venues, sports arenas, stores, at conferences, by transport companies, and by telecommunications companies. They are also used in advertising screens and by real estate companies.

As previously mentioned, beacons can be used by stores to send customers push messages about special offers when they are close to the store. For example, one telecommunications operator offered complimentary charging to passing customers when the dedicated app registered that the customer's phone was low on power. As mentioned, however, the use of beacons does not always result in a message to the user. The technology can also be used to map and record the customer's visits and movements in stores or shopping malls without any notification from the app.

Beacons may also be used to connect people's movements in real life with their presence online. *Retargeting* is when online advertisements are customised based on which sites the user has visited and what they did while visiting those sites. Until now, retargeting has been based solely on our movements online. With beacons, it is now also possible to offer online marketing based on our activities in the real world and which stores we have visited. There are companies that specialise in this type of solutions, but the Norwegian Data Protection Authority does not have the impression that those solutions are prevalent in the Norwegian market yet.

The app determines what the beacon signals will be used for. Therefore, beacons can be used for many different purposes in different locations. They can, for instance, be used in ticketing systems, for information on public transport, or to check in to planes or hotels.

Privacy implications

Tracking and compilation

Beacons can be used to determine our location through apps on our mobile phones. As beacons use Bluetooth technology, our location can be determined more accurately than by WiFi tracking. Over time, information from beacons can reveal our habits and interests. This is an invasion of our private lives. In principle, everyone has the right not to be subject to tracking of their movements nor unnecessary registration.

In order for tracking to be permitted, the individual must consent to it. Furthermore, the tracking must have a legitimate purpose and not be disproportionately invasive. For the user to be able to consent, they must also be given information about what the tracking involves: will beacons only be used to provide messages and advertisements, or will the user's movements be registered? Who is behind the tracking, and what is the purpose? Consent can be obtained and information can be given through the app. It is therefore important that the app be developed in both a user-friendly and a privacy-friendly manner.

Specific information must also be provided in locations where beacons are in use, for example by way of signs or other clear information sources. It will not always be apparent in the app where tracking occurs, and some apps can register beacons in many different locations, such as all the stores in a retail chain. The user is not always aware of this. This information will also benefit those who have not downloaded the app. Those persons would otherwise not have received any information, and as mentioned, operating systems and other applications

Example

In the summer of 2015, Kristiansand Zoo deployed beacons as a pilot project. Visitors that downloaded the zoo app were able to receive notifications about events in the park, such as the feeding of the lions.

The purpose of the project was to map the behaviour of the visitors in the park in order to improve service. By using beacons, the app could measure how long people stayed in one place, find out how they moved, and solicit feedback on the attractions. The zoo stated to the newspaper Stavanger Aftenblad (23/07/2015)* that tracking was based on prior consent of the visitors.

(*http://www.aftenbladet.no/nyheter/innenriks/Dyreparken-folger-gjestenes-bevegelser-3739737.html)

can potentially register beacons even though the app in question is not installed.

With beacons, our movements in the physical world can be connected to our movements online. The app can use beacons to determine our position and even at which store shelves we linger. At the same time, it may be connected to social media, customer clubs, or other services that know a lot about our habits and interests online. The app can also contain other information about us. This sort of compilation of personal data is particularly invasive.

As with WiFi tracking, beacons placed in certain locations can reveal our state of health, religious beliefs, political views, or sexual orientation. It is important that applications do not use information about us in a discriminatory manner, e.g. by providing offers based on assumptions about our solvency or ethnicity.

Some suppliers of beacons or beacon solutions may wish to use information from the beacons for their own purposes, such as to improve their services. This is a problem that may occur with Facebook's beacons – beacons that Facebook gives to businesses for free. When deploying a beacon, the company or business has the responsibility to maintain a complete overview of how personal data will be processed and to ensure that the information is not disclosed to others without the person's consent.

Security

It is a fundamental principle of privacy that personal data must be protected from unauthorized use. Beacons make it possible for our movements to be recorded by businesses other than those that deployed the beacon, such as developers of other apps and operating systems.

There are also other vulnerabilities affecting beacons that may challenge the right to data protection. Such vulnerabilities include:

- the inability to authenticate;
- cloning and copying;
- changes, hacking, and reprogramming;
- abuse.

It is possible to scan for beacons, read their IDs, and then create an app that can respond to the same IDs. It is thus possible to hijack users and provide notifications from competing apps. For example, a store may choose to give you an offer as you walk into a competing store.

Solutions for rotating beacon IDs, such as Google's *Ephemeral Identifiers*, may offer some remedy to this issue. This kind of solutions continuously changes the beacon's ID, and only authorized devices can use the signal.

As mentioned, some beacons send out URLs. It is possible to place malicious code in these URLs. Malicious code includes code that weakens the security of a mobile and makes it vulnerable to unauthorized access. It appears that the only way to prevent this kind of hacking of beacons is to ensure that apps that allow this kind of code to run are not approved in the app stores.

Disabling beacons?

When downloading apps, it will often be necessary to consent to beacons as part of the terms and conditions. If you do not want to accept this, your only options are to uninstall the app or disable Bluetooth.

Disabling Bluetooth altogether, however, is an *all or nothing solution*. For example, one might find some beacons useful, while wanting to avoid others. In addition, many people are not familiar with the technology and are thus not able to protect themselves. Some people use Bluetooth for other purposes, such as connecting a smart watch to their phone or listening to music using wireless headphones, and therefore cannot readily turn off Bluetooth. Furthermore, some operating systems will automatically enable Bluetooth after installing software updates or rebooting, without the user knowing about it. In other devices, such as cars, there may not be an option to disable Bluetooth.

The latest versions of mobile operating systems allow the ability to manage individual apps' access to different services, but these options are still not easy accessible to ordinary users.

Guidelines for the use of Beacons

1. Tracking using beacons can only take place if valid **consent** is obtained from the persons being tracked. For the consent to be valid, it must be made clear to the user how the tracking will take place, who the controller is, and what the purpose is. If tracking involves linking our physical and online movements, this must be clearly stated.

2. Consent can be obtained within the app. The consent must be separate from any other conditions, and it must be possible to withdraw the consent from within the app.

3. The **purpose** of the tracking must be clearly defined. The tracking measure can only be used in line with this purpose, and personal data collected cannot be reused for other purposes later.

4. It is unlawful to collect more personal data than is **necessary and relevant** for the purpose.

5. The controller must have **full oversight** of how personal data is processed. It must ensure that the information is not disclosed to others unless the person consents.

6. The application **cannot** use the information in a discriminatory or offensive manner.

7. **Avoid** using tracking technologies in locations that can reveal a person's state of health, religious beliefs, political views, or sexual orientation.

8. The controller must **minimize the possibility of abuse and implement security measures** that ensure that other businesses cannot make use of its beacons. Moreover, security measures must be implemented to protect the personal data so that it does not go astray.

9. **Information** must be provided in locations where beacons are deployed, using signs or other clear information sources. The information must include how the tracking will take place, who the controller is and what the purpose is. If the tracking involves linking our physical and online movements, this must be clearly stated. This information must also be included in any privacy statements.

10. There must be **clear procedures** for how long the information collected by the app is to be stored. The information cannot be stored for any longer than is necessary for the stated purpose.

11. **Notification** must be given to the Norwegian Data Protection Authority.

Intelligent Video Analytics

Intelligent Video Analytics (IVA) is technology that automatically analyses content from surveillance cameras. Video analytics may include registering what sort of objects are in the picture, triggering alarms based on where and how objects move, and recognising faces. This may for example be used to detect when someone climbs over a fence or removes a valuable object, to count people, or to analyse movements in shops and public places.

Put simply, video analytics is based on interpreting changes from one picture to another, i.e. changes in pixels in a stream of images. Video analytics is based on various sets of mathematical rules or algorithms. The analysis can be carried out on saved recordings or within the surveillance cameras themselves, which are often now equipped with processing power and software. Through video analytics metadata is generated, i.e. data about what appears or is happening in the pictures. Metadata about objects can typically include colour, direction, speed, and size, and whether the object is a vehicle or a human. The metadata is searchable.

Previously, it was necessary for a person to review surveillance footage for the content to be rendered usable. With intelligent video analytics, this is no longer necessary.

The word "intelligent" can be misleading, since we are not talking about artificial intelligence, but rather something that happens automatically. Several other terms are used for the technology – *Video Content Analytics* (VCA) and *Video Analytics* (VA) are used relatively synonymously.

Functionality

Intelligent video analytics offers various different features and is often aimed at specific areas of application as needed. It may therefore be useful to divide the features into three main categories.

Detection and tracking. With intelligent video analytics, it is possible to detect "new" objects, such as a person or a car, entering the picture. Any moving object is given an event marker and a time stamp, which makes it possible to track the object's further movements: where and how the object moves, its direction, speed, whether it stops and the time spent. Video analytics can also detect fire or smoke.

Describing objects. Video analytics can also register an object's characteristics (such as colour or size) or classify the object (for example, vehicle or human). Other characteristics may include temperature, estimated age, gender, and ethnicity. Video analytics can also provide more advanced object descriptions, such as categorizing a person's emotions using facial expressions. Furthermore, it is possible to automatically export all faces in the picture to a separate image database.

Identifying objects. Intelligent video analytics can be used for facial recognition. It is also possible to link a face to an already known identity in a blacklist or whitelist of individuals. The system may also be able to recognise the same face in other surveillance images, or across systems, without knowing the person's identity. The systems will probably also eventually be able to combine techniques such as facial recognition and gait to identify people.

Automatic number plate recognition (ANPR) can identify a vehicle's registration number in an image or video stream and automatically read and store the registration number as metadata. The systems may be based on dedicated cameras that are installed and adjusted especially to capture number plates (in a parking garage, for instance). It is also possible to analyse video from cameras that are used for other purposes. The cameras used can be fixed, mobile checkpoints, or mounted in vehicles.

Application

Intelligent video analytics and metadata can mainly be used in three ways. It is worth noting that these applications of video analytics may benefit very different purposes.

Automated alerts or alarms can be created based on predefined criteria. The criteria may include a person crossing a line or remaining in an area for more than two minutes, people starting to gather in an area, or a vehicle moving against the direction of traffic.

The recordings are **searchable.** For example, searches can be made to find large black cars travelling northbound within a specified timeframe. Previously, the only way to find relevant information was through time-consuming manual review of the surveillance tapes.

Statistics can be generated from the recordings, e.g. statistics on how many customers have moved through a given area or how the customers move within a shop. This is known as customer flow analysis. Customer flow analysis can also provide statistic on, for instance, the percentage of customers that are female.

Purposes

Traditionally, camera surveillance has predominantly been used for various security purposes, such as the protection of life and health and to prevent and solve crimes. In this regard, intelligent video analytics represents both continuity and a breach of continuity. The security purposes are still relevant, but new purposes and applications have also arisen. One particular use – or perhaps more correctly a handful of uses revolving around a common theme – stands out, namely fulfilment of commercial interests. The terms *customer intelligence* and advertising are key here. Video analytics can also be valuable for a third purpose, work management and planning.

Security. The features of intelligent video analytics are well suited for security purposes. A number of systems currently on the market are clearly intended for this purpose. These systems can offer predefined alarm rules that issue an alert whenever virtual boundaries are breached, moving objects are detected (theft detection), or "suspicious" behaviour takes place. They can be used for the security of both assets and people. Facial recognition software with the ability to search for faces in criminal databases can also be used for security purposes. The systems also make it easier to search for specific events after a security-related incident has occurred.

Commercial interests. Camera surveillance has traditionally not affected the bottom line of businesses beyond limiting losses caused by theft and vandalism. Intelligent video analytics changes that, and camera surveillance can now be used in different ways to help boost earnings. Tracking data on the presence and actions of individuals can be aggregated into statistics. By obtaining information about their customers, companies and businesses can optimise advertising and product positioning. In its advanced form, video analytics can form part of an effort to adapt physical advertising to customers' age and gender or to measure the effectiveness of advertising campaigns. Optionally, the system can identify an individual in a store as a returning customer or a new customer, which offers useful information about how the customer should be received.

Work management and planning. The triggering of an alarm is not necessarily in response to a security incident – alarms can also notify about queuing at the checkout or chaos in the parking lot. Intelligent video analytics can assist managers in detecting problems and manage resources accordingly. When do we need many staff, and when can we get by with just a few employees? Through good customer statistics, it is possible to know when there are many customers and when it is quiet. Visits can also be linked to other data, such as the weather, resulting in prediction models allowing staffing to be planned according to weather forecasts. Compared with security and commercial considerations, however, this purpose has been less central to development thus far.

The automated analysis of video content is not just about developing new tools for old purposes. The imagination is the only limit to what can be analysed from pictures and how that information can be used. The development is significant for the monitoring practices that already exist in society – the extent to which video surveillance is used, which purposes surveillance is used for, and how the surveillance equipment and recordings are used on a day-to-day basis. It is difficult to predict the full range of consequences over time.

Prevalence and usage

Security and commercial purposes

The Norwegian Data Protection Authority has examined the market for intelligent video analytics and been in contact with a number of companies and businesses that offer products and services related to the technology. Our impression is that the technology is on the rise, but not yet widespread. The technology appears to be used particularly for security purposes and commercial interests.

According to our research, most providers of camera surveillance equipment offer intelligent video analytics solutions. The providers point out that the technology is used, among other things, to secure property and assets outdoors. Video analytics is used on construction sites, in factories, in the recycling industry, and in conjunction with logistics and storage. What these areas of application share, is that the purpose is often to avert criminal acts or to safeguard life and health.

Intelligent video analytics has thus far been costlier than conventional camera surveillance, and therefore demand has predominantly come from larger businesses. However, several suppliers are emphasizing that prices are falling, which has led to growing interest among customers. Moreover, it seems that it is easier for businesses to justify the extra cost if it is also an investment in increased income – that is, if the technology also can be used for commercial interests. This demand is of great significance for the development of new products and solutions.

Examples of use

One of the companies the Norwegian Data Protection Authority has spoken to offers solutions that are especially suitable for security purposes. The company is currently working to develop several tools for customer analysis, as there is great demand for this. The tools will be able to identify customers' movements in stores and identify their gender and to some extent age and facial expressions. They will also be able to identify what kind of cars the customers drive, which can be used to draw conclusions about the customers' financial status. This information can be utilised to measure the impact of sale campaigns or to customize stores, goods, and offers to the customers.

One company is working to develop intelligent video analytics solutions that can be used in the healthcare sector.

In another case, video analytics tools are being used exclusively to secure infrastructure in the power industry.

There are solutions for customer analysis based on information from thermal cameras or other sensors rather than regular surveillance images. These tools can thus generate much of the same information while the privacy implications are reduced compared to the use of ordinary footage. This does not, however, mean that the data is anonymous. In some contexts, typically in the workplace, it will be possible to identify individuals even if they cannot be recognized based on how they appear in the images. For example, an employee in a shop can be easily distinguished from customers based on where the person is located, how they move around within the location, and how long they are present.

Individuals can also be identified if information from thermal cameras is linked to personal data from other sources, such as the use of access cards or loyalty cards. In this case, the material will constitute personal data. It is therefore important to note that fixed thermal cameras can be considered surveillance cameras, which means that the specific legal provisions on camera surveillance apply. These provisions contain duties regarding signage and deletion of footage, among other things.

Intelligent video analytics can also be combined with advertising boards. The cameras will be able to analyse passers-by and provide advertising tailored to them.

Examples of use

At Copenhagen Airport, Kastrup in Denmark, advertisements are displayed on screens based on information about travellers from the Amadeus reservations system and from interviews, for instance that business travellers often travel at certain times or from certain gates. Cameras are mounted next to the advertising screens to see if passers-by are looking at them. These cameras are also able to analyse gender and the age group to which the persons belong. In the long term, the intent is to use this video analysis to customize the content on the screens to the person or persons who are passing by at any given time.

Similar video analytics solutions have been used in Norway in advertising campaigns for companies such as Chess, KappAhl, Coca-Cola, Sony Music, DNB, and Oreo Mondelez.

Automatic number plate recognition

Automatic number plate recognition is used in both the public and private sectors.

The police, the Customs Service, and the Norwegian Public Roads Administration all use number plate recognition to check cars against other registers and control vehicles with deviations. For example, vehicles for which annual fees or insurance have not been paid are stopped. Both fixed installations and mobile checkpoints are used. The technology is also used for toll collection. It may furthermore be used in traffic enforcement cameras and to measure the traffic flow to provide information about driving times and route suggestions.

Some parking companies are currently using this technology to register vehicles driving in and out of parking spaces and garages. This information is used to invoice customers or check that payment has been made. In addition, automatic number plate recognition can be used as access control in parking lots and garages by only opening the gates or barriers if the vehicle's registration number is on the list of approved numbers.

Privacy implications

By means of intelligent video analytics, we are both recorded and analysed. The potential for violation of privacy is therefore greater than for conventional camera surveillance. The system can draw conclusions about individuals even without anyone looking at the recordings. Video analytics can see if we are standing in one place for a long time, map which store shelves we visit, or register where we drive. This generates information about our behaviour and our habits. Intelligent video analytics also enables tracking over location and time as some systems can recognize faces or number plates.

Everyone has a certain right to move without being traced, and the right to privacy also applies in public places. If it is not necessary to register identifying data, individuals have a right to anonymity. The purpose of the collection of personal data must be specified, and the collection and use must be restricted to the defined purpose. It is important that no more data be analysed than is strictly necessary, so that the privacy and integrity of individuals are preserved as much as possible. Moreover, all collection of personal data must be proportional to the purpose, so that there is a balance between the interest of the company and the privacy of the individual.

It is important to be aware that intelligent video analytics is a form of camera surveillance and that the rules governing camera surveillance apply to it. Until now, surveillance cameras have mainly been used for compelling purposes, such as crime investigation or the protection of life and health. For the most part, recordings have been short-lived and only disclosed to the police. With intelligent video analytics, there are more reasons to set up surveillance cameras in new locations or use existing cameras for multiple purposes, since cameras can collect valuable customer data. It may be beneficial to store this data for longer and use it differently than traditional recordings. The rules for camera surveillance limit when, where, and how camera surveillance and recordings can be used.

It is a basic principle that individuals are entitled to information when their personal data is processed. It is therefore important that information be given when a location is subject to camera surveillance. Intelligent video analytics, however, involves more than what people normally associate with camera surveillance. Where video analytics involves facial recognition or number plate recognition, for example, it is important that information on this be provided so individuals understand how their personal data is processed.

Where video analytics is misused, discrimination may ensue. The cameras can be set to trigger alerts if people with certain characteristics are present. Examples of such characteristics include colour, age, and whether the vehicle the person is driving is expensive or not. Information on race or ethnic origin belongs to the special categories of personal data. This data is therefore subject to strict rules as to when it is permitted to process it.

Nonetheless, video analytics have certain privacy advantages. When an incident occurs, it will be possible to jump straight to the event without having to go through the entire recording. Consequently, most of the recording will remain unseen until it is deleted. The technology itself is not necessarily the problem – it is the use of it that may raise issues. If intelligent video analytics is employed in a privacy-friendly manner and in accordance with the law, it may prove to be a useful tool.

Guidelines for the use of Intelligent Video Analytics

1. Cameras with intelligent video analytics can be used only when camera surveillance is otherwise permitted. Intelligent video analytics must have a **compelling purpose**, such as the prevention or investigation of repeated or serious crime, or the protection of life and health. It is normally not permitted as a tool for collecting customer data. The use of video analytics must be proportionate to the privacy implications and the purpose.

2. The purpose of video analytics must be clearly defined. Intelligent video analytics can only be used in accordance with this purpose, and metadata or personal data cannot be reused for other purposes later.

3. It is unlawful to collect more personal data than is **necessary and relevant** for the purpose.

4. There must be **clear procedures** for the analyses, the alarm criteria and searching the metadata. The analyses should not be too intrusive, and it is not permitted to analyse more than what is relevant and necessary. For example, it will normally not be necessary to analyse gender and age.

5. Video analytics cannot be used in a discriminatory or offensive manner, for instance by setting alerts for when individuals of a particular skin colour are present.

6. **Avoid** using tracking technologies in locations that can reveal a person's state of health, religious beliefs, political views, or sexual orientation.

7. Automatic number plate recognition can be used in commercial parking lots provided that it is possible to pay the parking fee on the spot and that the number plate information is erased when payment has taken place.

8. **Security measures** must be implemented to protect the recordings and metadata so that they do not go astray.

9. **Information** must be provided whenever an area is subject to camera surveillance, using signs or other clear information sources. If facial recognition or automatic number plate recognition is taking place, this should be included in the information. The information must also include who the controller is and include the controller's contact information. If audio recordings are made, this must also be stated. This information must also be included in any privacy statements.

10. **All recordings must be erased** when storing them is no longer necessary for the intended purpose, and no later than seven days after recording. If it is likely that a recording will be turned over to the police, the recording can be stored for up to 30 days. Recordings from postal or bank premises, including footage from counters at in-store banking or in-store postal facilities, can be stored for up to three months.

11. Metadata from intelligent video analytics must be deleted along with the recordings from which the data originated.

12. Statistics can only be developed as long as it is in accordance with the defined purpose and justifiable with regard to the balancing of interests of the business or company and the individual. One can thus not use security related monitoring to extract customer statistics. The statistics can be stored freely as long as the data is completely anonymous, for instance how many times a specific security incident has occurred within a given period. The specific data on which the statistics are based cannot be stored longer than the recordings (see the above point concerning metadata).

13. **Notification** must be given to the Norwegian Data Protection Authority.

What comes next?

In this report, we have written about four technologies that are used to track us in public spaces, but there are several additional technologies that we believe will affect our privacy in the years to come.

RFID (Radio Frequency Identification) is a technology that utilises chips able to receive and respond to radio frequency signals from an RFID reader. RFID is currently used for many purposes, including securing goods in shops, in travel cards, or in toll tags. In clothing stores, RFID tags are attached to clothing, but researchers have now developed a method that makes it possible to weave RFID tags into the fabric of the garment itself. This may deter theft by making it impossible to remove the tags, but at the same time, any store could monitor how customers move through the store, without their knowledge or ability to refuse. Furthermore, it may be possible to track RFID tags over long distances depending on the chosen standard. Poor security of RFID tags in access cards, payment cards, passports, or the like may provide an opportunity for wireless data copying.

One innovation mentioned in this report is the use of **audio tracking** to identify users across the various platforms they use. An example of audio tracking is where commercials on TV and the internet plays a high-pitch sound that is inaudible to humans, but that is registered by the user's mobile phone. Information about which commercials have been registered can be passed on to marketers, who can identify which commercials we watch, how long we watch them, and if we later search for the product in question on the internet.

As of today, most surveillance cameras consist of one camera with one lens, but this is about to change. Prototype cameras consisting of **many micro cameras looking through the same lens** are being developed. The resolution of the surveillance images can be as high as one gigapixel (1,000 megapixels). In comparison, the camera on an iPhone 6s has a resolution of 12 megapixels. The consequence of this is that one can obtain extremely detailed images of large areas. It would for example be possible to take a snapshot of a football stadium, or even an entire city, and be able to identify individuals within it. This in itself is an unpleasant thought. Seen in conjunction with the ever-improving speed and accuracy of video analytics, the potential for intrusive surveillance is dramatic.

Summary

Information collected through the use of tracking technologies can be of great value, both commercially and for society. For example, both intelligent video analytics and RFID can be used to prevent crime. WiFi tracking can be used at airports and other locations to ensure a smooth flow of passengers. With beacons, businesses can offer new services and improve day-to-day productivity. The technologies themselves are not the problem – as long as they are used in accordance with the privacy legislation.

Privacy challenges arise as a result of how the technologies are used. When tracking technologies are employed, we are often provided with inadequate information. With information about how our personal data is processed we are able to make informed decisions and protect our privacy. Information and transparency are therefore essential for the future and can be achieved without using a lot of resources. Businesses that provide proper information on how they process personal data and show that they take customer privacy seriously, may gain a competitive advantage.

Privacy has been high on the agenda in recent years. In 2018, new and stricter privacy rules will be introduced in Norway through the adoption of the EU's new General Data Protection Regulation. The rules will reinforce the obligation to provide clear and accessible information. Furthermore, privacy by design and default will become a requirement, meaning that privacy must be taken into account during all phases of development of new systems or solutions. This is both cost-effective and more efficient than making changes to a completed system. The aim is for new solutions to be more privacy-friendly, so that technology and privacy can operate in conjunction.

Datatilsynet

The Norwegian Data Protection Authority

P.O. Box 8177 Dep.,
N-0034 Oslo, Norway

Visiting address:
Tollbugata 3, Oslo

postkasse@datatilsynet.no
Phone: 00 47 22 39 69 00

Datatilsynet.no
twitter.com/datatilsynet