




you decide ...

Thoughts and facts about protecting your personal data



This brochure has been published by The Data Inspectorate in cooperation with the Norwegian Directorate for Education and Training and the Norwegian Board of Technology, January 2007

ISBN 978-978-82-997509-0-5

Translated to English by: SDL Norway AS

Editor in chief: Ove Skåra, The Data Inspectorate

Project manager: Guro Skåltveit, The Data Inspectorate

Journalist: Inger Lise Welhaven

Concept/produktion: Gambit Hill & Knowlton

Design: Haugvar Communications & Design

Photography: Håvar Haug/Bård Ek

Illustrations: Åsne Flyen

Printing: Nor Grafisk AS

For more information, go to www.dubestemmer.no

**The Data
Inspectorate**

P.O. Box 8177 Dep
NO-0034 Oslo
Tel: +47 22 39 69 00
www.datatilsynet.no

**Norwegian Directorate for
Education and Training**

P.O. Box 2924 Tøyen
NO-0608 Oslo
Tel: +47 23 30 12 00
www.udir.no

**Norwegian
Board of Technology**

P.O. Box 522 Sentrum
NO-0105 Oslo
Tel: +47 23 31 83 00
www.teknologiradet.no

YOUR CHOICE

This brochure underlines the importance of protecting your personal data. It shows you how your personal details can be used and abused by others, and how you can protect this information.

You'll already be familiar with some of the content other bits will likely be completely new to you. We hope this brochure will help with discussions – and perhaps introduce you to new concepts. Our goal is to help you make the right choices.

You decide.

The parent-teacher-student
conference went ok ...



... but all hell broke loose when the teacher googled my work!

You don't show up to the parent-teacher-student conference and admit to taking your essays straight from the Internet. And you're not likely to raise your hand in class and tell people what websites you've been on recently.

If you have a secret to tell your friend, you're hardly going to advertise it on flyers in the cafeteria. And if you're chatting with your girlfriend in your room, you don't ask your visiting aunt to come and join you.

Maybe you'd rather keep things to yourself ...

But then you aren't always as anonymous as you think.

BANG! The door slams again. You're finally alone. You sit down in the chair. Turn on the computer. Chatting with your friends and surfing online. Left to your own devices, away from annoying parents and curious younger siblings. And if they absolutely have to come in, they must knock first. While in your room, you rule the roost.

"PROTECTING PERSONAL DATA IS ALSO A QUESTION OF OBSERVING THE UNWRITTEN RULES FOR GOOD MANNERS. WE DON'T LOOK THROUGH KEYHOLES, WE DON'T OPEN LETTERS WE FIND ON THE STREET AND WE DON'T TELL OUR JOGGING PARTNER ABOUT OUR SPOUSE'S CANCER DIAGNOSIS."

Georg Apenes, The Data Inspectorate

You are entitled to be left in peace

We all have things we don't want to share with other people. Not because they are illegal or because we need to keep them hidden, but simply because it's our own private business. This is why you are the one who decides what other people find out about you from the outset and what information you choose to keep to yourself.

Your choices

You alone decide what you want to share, and who with. Very few people will want to ask out loud for a Chlamydia test when they're standing at reception in the doctor's surgery – especially not with a full waiting room acting as an attentive audience. Few people will circulate images of themselves naked via MMS and risk that five seconds later the very same images will have reached their boyfriend or girlfriend, teachers and parents. No one likes it when other people snoop around their private things, whether it be in their bedside cabinet or on their computer.

Your boundaries

The need to have your own personal space – which others respect and don't barge into – varies from person to person. Different groups of friends also have different understandings of what is private. What's more, attitudes about what is private have changed. Things that your parents may only ever have done behind closed doors are perhaps things that you wouldn't think twice about showing everyone.

Sometimes we need to be any-

mous. We should be able to feel secure in the knowledge that no one else is able to know everything about us, or see everything that we do. This is why you can go to the school nurse without others finding out what you talked about. You should also be able to go to the bathroom without being recorded on camera.

You have the right to shut the door and decide for yourself who you invite in.

WHAT DO YOU THINK?

Where do the boundaries lie for what your parents should have the right to know about you? Should they be able to see what you keep in your bedside cabinet? Should they be able to see your bank statements to check how you are using your debit card? Is it ok that they go onto your computer and check which websites you've visited?

How old should you be before your parents are no longer able to demand access to information about everything you do? Should there be different limits for the examples listed above, and if so, how should these be defined?

TASK:

Attitudes about what is private and what is appropriate for public consumption have changed.

Find examples of situations shown on TV, online, in newspapers and magazines that you think could not have been shown 20 years ago, because they would have been considered "private" back then. Show how the boundaries have changed. Where do you think the boundaries should lie today?

The Personal Data Act

The Personal Data Act is intended to ensure that information about you is used in a way that is respectful of you. The purpose of this Act is to protect people from having their right to privacy violated through the processing of personal data.

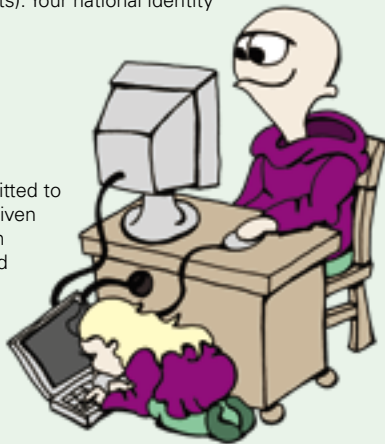
Personal data

An item of personal data is an item of data that can be linked to an individual person. For example, this means that a name, age, address and telephone number are items of personal data if they can only be linked to you. Images that can be identified as a certain person are also a form of personal data, even if no name is attached to the image.

Your national identity number consists of your date of birth (the first six digits) and your personal number (the last five digits). Your national identity number is an item of personal data.

Consent

As a starting point, other people are not permitted to use your personal data unless you have first given your consent, i.e. you've agreed to allow them to do so. Your consent should be voluntary and given willingly, and can be withdrawn at any time. This is the general rule, but there are exceptions. For example, in a number of contexts, the central and local governments are allowed to record and use your personal data without your prior approval. The general rule is that once you have turned 15, you can agree to the collection and use of your personal data. If you are younger than this, anyone who wants to use your personal data must generally obtain your parents' consent. If sensitive personal data is involved (such as criminal acts, health, sexuality, etc.) your parents' consent is often required until you reach 18.



Information and access

- If you give out your personal data, you have the right to know who is collecting this data, what it will be used for, whether it will be transferred to other people and if so, who will have access to it.
- You have the right to know what data other people hold about you, what the information is going to be used for and how they have obtained the information.
- You can request that incorrect or incomplete information be corrected.
- Data that is no longer required for the original purpose should be deleted.

THAT'S LIFE!

With dad in tow

A teenage girl went on a ski trip with friends and without her parents. But was she really on her own? Her father subscribed to the mobile phone-based security monitoring service Trygghet-smobilen, and sat at home in front of the computer, keeping an eye on where she was. He didn't see anything wrong with this kind of monitoring, and his daughter said she thought it was ok, although she was a little skeptical about the fact that her father could trace her at all times. The Ombudsman for Children in Norway, Reidar Hjermand, was extremely skeptical. In his opinion: "A system where parents can check where their children are at any time is an obvious violation of the child's private life."

Source: NRK Dagsrevyen

Monitoring her daughter's spending

One mother explains that she puts her daughter's allowance into a bank account using a debit card rather than giving her cash. She regularly goes through her daughter's bank statements online, and thereby has a complete overview of when and where her daughter has used her allowance.

Source: The Data Inspectorate

SCHOOL IS TERRIBLY BORING – now and then. It can be very tempting to duck behind the screen and find something more fun. But even if you're sitting in a corner and no one is looking over your shoulder, there are a lot of people who can see what you're doing.

**"PERSONAL DATA PROTECTION
IS BASIC PROTECTION
OF THE PRIVATE LIFE OF THE
INDIVIDUAL"**

Do you know who's watching?

Surfing and chatting feel private, so most people want to be left to sit in peace. Preferably at home, with the door shut, maybe even locked, just to be on the safe side. It's easy to forget that the door is often wide open in the world of technology.

Easy to check

In order for the e-mail you send to reach the right person, and for the websites you visit to be sent to "your" computer, your computer is assigned an electronic address (an IP address). Most schools have a firewall which protects against break-ins by hackers and viruses, and which also makes it possible to see which computer has which IP address, which websites each computer has visited, how many times and for how long.

All the websites you visit are also saved on the computer in the browser's history file. This is saved to make it easier the next time you want to visit the same site. If you don't delete the history file on the computer, it is easy for other people to monitor your time online. Unauthorized people may also be able to access e-mails you have sent and received. If friends, or people who aren't such good friends, get hold of your password, they will have access to everything that is intended for you and you alone. It can be both unpleasant and embarrassing.

Responsibility and rules

It often doesn't matter so much if other people see what you have done over the course of a day or during an hour-long

class. But there may be times when this isn't ideal. This is why your school has rules about what students and teachers are allowed to do on the school's computers. There are limits on what the teacher can monitor in terms of your activities on the computer and via the firewall, but at the same time, you are expected to take responsibility for your own activities.

When you're online, it isn't always easy to know whether or not someone

is spying on you. When you're alone with your computer, you may feel anonymous, and it's easy to think that no one can see what you're doing. That's not how it works ...

You aren't anonymous online.

WHAT DO YOU THINK?

Who should be able to access information from the computer you use at school?

Teachers? Classmates? Parents? What should they be able to see, and how should they be able to use this information? If the school discovers that bullying is going on via the school's network, should the teacher then be able to go into the system and check what's going on and who's behind it?

TASKS:

Talk with other people in your class. Help each other figure out how you can:

- delete the history file in the browser
- delete all temporary files ("temporary Internet files")
- change the privacy settings in the browser

What rules apply at your school when it comes to using computer equipment?

Find out whether the school has rules covering teachers' rights to access information about what you do on the computer. What do you think your teachers and the school should or should not have the right to check? Make suggestions for rules and discuss them in class, or take them up with the school via the student council.

Like an open journal

Other people are able to see which websites you've visited, either by checking the history file or temporary files for text, images and e-mails. These files are not automatically deleted when the browser is closed. If you don't delete the content yourself, other people can snoop around your online activities.

The danger that other people will try to access the information you leave behind may be greatest when you use computer equipment at school, in the library or at an Internet cafe.



How can they know who I am?

Every time you go online you are assigned an IP address. The Internet service provider records when you are connected and which IP address you have been assigned. The websites also record the IP addresses that visit them. When the police want to investigate who has visited a website, they can check the website's logs and then ask the Internet service providers for a list of who was using the IP addresses at a given point in time.

Many websites are interested in knowing who visits them, so they save a little file (a cookie) on your computer. Each time you visit the website, it checks whether your computer has such a cookie file, and records the information in it, for example the username and password used to log in to the website. You can refuse permission for websites to save cookies on your machine by adjusting the privacy settings in your browser. But then you risk some websites not working properly. You must decide what is most important: protecting your personal data or accessibility.

What does your school have the right to check?

As a general rule, the school may not use the computer system's log function to monitor students' Internet use. The purpose of the log is to ensure responsible operation of the computer system. Therefore, the log may be used to uncover unwanted online activity. In such instances, the school may use the information in the log to send out warnings that this Internet activity must stop, and that if the activity continues, the school will use the log to investigate who is involved.

The school itself must define what constitutes unwanted Internet activity. Any monitoring of students' online activities must occur in line with the regulation on e-mails, once this has been adopted by the authorities. In the meantime, it is important that the school develops clear guidelines that students can use to orientate themselves.

THAT'S LIFE!

Caught on the school network

At a school in Eastern Norway, the online learning platform "It's learning" was abused by some students. A number of bullying messages containing swear words were recorded in the chat room. The use of nicknames made it difficult to identify the sender, so the chat room was closed to everyone. But the problems continued via e-mail. The head teacher also discovered that passwords and usernames were being stolen. Subsequently, those involved were caught and several students were banned from sending e-mails.

Source: Romerikes Blad

Teachers snooping around on students' computers

Students at a number of schools have raised the alarm about teachers engaged in unlawful surveillance and monitoring. In some instances, the teachers are said to have mapped out every move individual students made online by going through the logs in detail.

"This is of great concern. Teachers are not authorized to engage in this kind of surveillance", explains Halvard Hølleland, former head of the school student union of Norway (SUN). In his opinion, schools' supervision activities go too far, and thereby imply that students can't be trusted. Hølleland understands that there may be grounds for checking that the written and project work, submitted by students, is original and not taken straight from the Internet, but rejects the way in which this is being done.

"Instead, students should be required to create proper reference lists", he suggests.

Source: VG

A photograph of two young boys sitting together, looking intently at a laptop screen. The boy on the left has blonde hair and is wearing a grey hoodie with a black and white checkered collar. The boy on the right is wearing an orange baseball cap and a grey hoodie over a colorful cartoon t-shirt. A soccer ball is visible in the lower-left foreground. The background shows a wall with some posters. The text "It was just a joke ..." is overlaid in white, stylized font across the middle of the image.

It was just
a joke ...

... but suddenly I had
pressed “Enter”!

You don't pass out signed photos of your girlfriend to men
you don't know, saying “pretty fit, don't you think?”

If you film everything that happens at the end-of-year party,
you don't give the video to your dad for Christmas. And if
you hear something nasty about a guy you know, you don't
try to improve your reputation by informing the police, your
teacher or the other blokes at school.

Probably not ...

You decide what other people are allowed to know.

HI! HERE I AM! LOOK AT MY WEBPAGE! LOOK AT ME! ON MSN SPACES! ON YOUTUBE! ON PICZO! LOOK AT ME! VOTE FOR ME!

The Internet is fantastic. It offers an ocean of opportunities: you can create your own webpage and visit other peoples', download music and movies, chat with friends on MSN, share images and intimate secrets. But the Internet is also merciless. Once something's been said or done, it's too late to hit the "Undo" button. It doesn't exist.

You are your own editor

We all need to be noticed. Some people sign up for reality TV shows. Others create a webpage or blog where they post images and information about themselves. Whichever you choose, you'll get attention, both from people you know and people you don't.

A big responsibility

All newspapers have an editor, who is responsible for everything the newspaper prints or posts online, both text and images. Deliberate lies, slander, illegal images and racism can do great harm and lead to fines or imprisonment. The press has also developed a set of ethical guidelines for journalists and editors to follow, called "The Code of Ethics of the Norwegian Press."

Just like a newspaper editor is responsible for their newspaper, you are responsible for everything you post online. So you need to think about what you post online as far as your own personal information goes, and not least information about others. This also applies to images. It is equally important to be able to take responsibility for what you post on blogs and other websites. What may be a joke to you at the time, may be seen as harmful to others.

Too late to undo

It can be fun to post information and images of yourself. Sitting in front of your computer at home, it may seem innocent and not in the slightest bit dangerous. In this

WHAT DO YOU THINK?

Have you ever regretted posting something online about yourself or others, and if so, why did you regret it?

Why do you think someone might decide to post images of themselves on websites like deiligst.no, Piczo and MSN Spaces?

TASKS:

Enter your own name or your online nickname in the search field of a search engine.

- What did you find?
- Do you feel it presents an accurate image of who you are? Why/why not?

Get a copy of the Code of Ethics of the Norwegian Press. Create your own Code of Ethics with guidelines for what you post online.

environment, it is particularly easy to shift the boundaries between what is private and what you choose to share with others.

Once text and images are posted online, they are difficult to delete, and it is almost impossible to prevent them from being copied and circulated. Images of and information about you can end up on websites you didn't even know existed, and which you wouldn't really want to be connected with.

Think before you press "Enter".



Forever and ever

It is possible to delete information and images that are posted on the Internet, but sometimes it is impossible to ever delete them entirely. Someone may have downloaded the information and images, the information may already have been posted on other websites or copies may have been stored by a variety of search engines.



A real YES!

Each time you upload images of one or more identifiable people online, you must first ask their permission, and receive a real YES in response. A yes given at one point in time won't always hold true. If someone who said yes changes their mind at a later date, you are obliged to help remove the image.

Get rid of it!

This is how you delete unwanted information about yourself online:

1. Talk to the person who published it

Can you see who posted the unwanted information about you? Contact that person and request that the information be deleted. The sooner the better.

Still having problems?

2. Talk to the Internet service provider

Contact the Internet service provider's abuse team: they will usually be able to help you. You'll find the team by contacting the owner of the domain name (for example, online.no). To find out who owns a Norwegian domain, go to the Norwegian WHOIS database at www.norid.no.

Serious problems?

3. Contact the police

If you think the information is so extreme that it should be removed immediately, you should contact the police where you live. Report the situation!

Problems that aren't quite so serious?

4. Contact The Data Inspectorate

You can contact The Data Inspectorate for advice on removing unwanted information online. The Inspectorate can also help you with other issues with regard to protecting your personal data.

THAT'S LIFE!

Discovered her image on a Nazi website

A girl posted images of herself on a website where she met frequently with like-minded friends to exchange photos and tips about photography. A few months later she found an image of herself on a racist website. Under the title "Norwegian beauties" there were images of 122 girls (including herself) who knew nothing about the site, with the text "Images displayed for everyone who loves the Nordic race ...". Several of the images were taken from the same website. The images were there for several months without the girls knowing about it.

Source: The Data Inspectorate

"I can't take any more"

Last summer my friends and I partied a bit – like most other teenagers. We had a really good time and met new people. We took photos and posted them on a webpage. We had a password and everything! Nothing could go wrong. But when school started again, a lot of people heard that it was a "party site", and people became more and more eager to get the password. Then something terrible happened with the website where we had uploaded the images. Suddenly everyone could see the "owner's" pages. The nightmare started when the people we knew told their parents. In the end, one mother contacted the school and explained everything. We had to talk to teachers and counselors. My parents were also contacted, but fortunately they thought it was just part of being a teenager. It was worse seeing the other students. They knew something, all of them did. When I started school a year ago, I had a great time. But now I dread going to school every single day. I have learned a valuable lesson – I won't ever post something on a website, whether it's images or something else. Now I feel like I have a video camera following me. Regards, anon.

Source: Aftenposten, reader submission in the comment section Si ;D (abbreviated)

Stripped in front of the whole world

A 14-year-old girl posed for her boyfriend in front of a webcam. A couple of weeks later everyone could see her on YouTube. What had been an innocent bit of fun turned out to be a complete nightmare. Within 19 hours, the clips had been watched by 600 people. The girl's father reported the distribution of the images to the police, and the police are investigating the case.

Source: Expressen.se

WATCH OUT FOR THE MAN IN THE RED CAR! His name is Hansen and he's a rapist. Pass it on, watch out for the man in the red car, his name is Hansen and he's a rapist. Pass it on, watch out for the man in the red car, his name is Hansen and he's a rapist. Pass it on, watch out for the man in the red car...

Someone can STEAL your reputation!

Most things spread like a bushfire via text messaging. It is entirely possible that Hansen is a rapist. Maybe it is important to watch out for him. But who sent the first message? Is it ok to forward it? Might it be that Hansen isn't a rapist at all, but just stole someone else's girlfriend, and that someone is now out to get revenge?

Impossible to stop

Once a rumor has been started, it isn't easy to stop. Once an image has been sent from your mobile, there's no "Undo" button. Once you log off MSN, it's too late to say you didn't mean what you wrote. When the false allegations you posted online about the school's most hopeless teacher are read by the teacher's colleague, you could end up being punished under the Criminal Code.

For most people, a life without the Internet and a mobile phone is unthinkable. The world is getting smaller and circles of friends are getting larger. Mobile phones and the Internet offer us fantastic opportunities, which previous generations never had. But they also give us unprecedented opportunities to hurt each other. Research has shown that bullying online and via mobile phone is a significant problem among young Norwegians.

Students egg each other on to fight in the school yard. Someone films the whole thing with their mobile phone and then posts it online. The guy who's drunk the most at the party is convinced into stripping in front of the camera. The next day, the whole world can access the images both online and by mobile phone. A

WHAT DO YOU THINK?

Some people say that the Internet and mobile phones have made it easier to bully other people. What do you think?

Think back to messages and images you have sent or forwarded. Might any of these have offended other people, and if so, how?

What might you have done and said online that you would never have done in the real world?

Have other people ever posted information about you online? If so, did you like what you saw? Did they ask for your permission first?

TASKS:

Go to Piczo, YouTube or a similar site. Are there videos or images there that could be damaging to others and shouldn't have been shown?

Check your own or a classmate's website/blog. Is there information there that you think hasn't been approved by the person mentioned or photographed/filmed?

former friend "steals" Kari's identity and sends an unpleasant text message to their group of friends, with Kari's number listed as the sender. There is no more effective way to spread a message than online and by text message. For good and ill.

Think for yourself

When you are sitting in front of your computer or standing with your mobile phone

in your hand, you're the one who decides what you want to share with the rest of the world. You are responsible for thinking it through before you send or forward information and allegations about other people.

If you wouldn't consider doing it in real life, you shouldn't do it in the digital world either.

PROTECTING PERSONAL
DATA MEANS THAT
THERE ARE BOUNDARIES
AND RULES FOR HOW
OTHER PEOPLE CAN USE
INFORMATION ABOUT YOU.

Digital bullying

- 67,000 (14%) of Norwegian children and young Internet users between the ages of 9-16 have sent malicious messages online.
- 75,000 children and young people have received an e-mail that has troubled or frightened them. Of these, 19% have informed an adult and 10% have contacted the police.

Source: SAFT Barn Norge 2006



False sender

The messages you receive on your mobile phone aren't necessarily from the person you think they're from. There are in fact online services that make it possible for anyone to send text messages from whatever sender number they choose to specify.

Sending joke messages from a false identity isn't illegal in itself. It's what the messages are used for that decides whether a criminal act has been committed. Something that might be considered as a joke by one person could be seen as a real threat by another.

THAT'S LIFE!

Punished for online bullying

After having called another girl a "whore" in an online chat room, a 17-year-old girl in Eastern Norway was convicted of having disturbed the peace of another. The court considered that the message could be classed as public harassment and bullying and should, therefore, not be protected under "freedom of expression". The girl was ordered to pay a fine of NOK 4500. "We always find out who is behind this kind of harassment. People think they are anonymous online, but you always leave behind electronic tracks", the owner of the website said.

Source: *digi.no*

Fights on video

A fight is in full swing in the school yard. Two students are letting each other have it, egged on by the other students. Gradually, more and more students come to watch. Many are holding their mobiles up in the air. The fight is being filmed. The videos are uploaded onto YouTube.

Every day hundreds of thousands new videos are uploaded onto YouTube. Several show Norwegian students involved in fights. YouTube receives more than 250 million hits a month and videos like these are watched by thousands of viewers.

It is illegal to post videos online without the consent of those involved.


Source: *Dagbladet*

Hate site about Idol participant

When the Idol participant came home from the contest, she discovered that two classmates had created an online hate site about her. Among other things, visitors were encouraged to post very condescending and unfavorable comments about the Idol participant.

"The comments were just unbelievable. What's more, the website included a chat page where people could discuss everything about me. Such things are hurtful to read and completely impossible to defend yourself against. But the worst thing was that it was started by people from my own school", says the 18-year-old, who in hindsight regrets not reporting the incident to the police. The head teacher at the school reinforces the fact that bullying is completely unacceptable. The website was removed, and the boys responsible were punished by having their conduct grades lowered.

Source: *Bergens Tidende*

A black and white photograph of a man in a workshop. The man is wearing a light-colored long-sleeved shirt and pants, and is sitting on the floor, leaning back with his head tilted upwards and his mouth open in a shout or yell. He is positioned in front of a workbench. On the workbench, there is a calculator, a pen, and some papers. A woman in a puffy jacket is standing behind the workbench, looking down at something on the counter. In the background, there are shelves with various items, including a snowboard and some boxes. A digital clock overlay in the upper left corner shows the time 1:12:08:07.

1:12:08:07

Cool stunt at
the time...

... but I had forgotten the surveillance camera in the corner!

You don't send a video of your stunts and questionable actions to the police to improve your record. You don't sit with the door open in the bathroom cubicle at the shopping center.

When you're in the changing room at the clothes shop you don't shout "Hey, look at me – I'm not wearing any clothes!" to the people who work there. And if you had downloaded music illegally from the Internet, you're hardly going to send a letter to the record company saying "I nicked this one!"

Not if you had the choice ...

Do you always know who's watching?

ZIP UP YOUR ZIPPER. Rub the sleep from your eyes. Don't pick your nose whatever you do. Check your hair's ok and that your trousers are properly adjusted. Smile! The cameras are rolling – you're on!

"EVERYONE HAS THE RIGHT TO EXPECT HIS PRIVATE AND FAMILY LIFE, HIS HOME AND HIS CORRESPONDENCE TO BE RESPECTED."

From the European Convention on Human Rights

Safer with cameras?

The video cameras are following you. When you sit on the bus. When you're hanging out at the shopping center. When you're checking out the latest stuff at the clothes shop. When you buy a kebab from the van. When you are wandering around the city center, and maybe also when you enter the gym.

Insecurity is an important reason for surveillance being used in more and more places. Most bus drivers and passengers feel more secure if they know that a surveillance camera has been installed in the bus. The person standing alone behind the counter at the petrol station late at night is reassured by the fact that the area is under video surveillance.

Always a positive thing?

Video surveillance can help prevent and solve crimes such as vandalism, violence and theft. But it is important to think carefully about the consequences before a decision is made to install video surveillance, whether on the bus, at school or in a pedestrian area. Why is surveillance needed? Does it provide increased security? Can surveillance have negative consequences? Are there other solutions that provide as much or perhaps even better security?

There are no statistics suggesting that the general crime level decreases as cameras are installed. Instead, the violence changes shape or is displaced to other locations. People that are drunk or high on drugs, or mentally ill people, are not affected by the fact that there

are cameras present. This is why there is disagreement over the extent to which video surveillance contributes to a more secure society. It is also difficult to know how we – as humans – are affected by being under surveillance.

Not always reliable

In some instances, video surveillance can result in misunderstandings. In some places, cameras are used to discover unwanted individuals, who are then requested to leave the premises, even if they haven't done anything wrong. In order to avoid misunderstandings or abuse, it is important that those who install such

cameras know how it is supposed to be done, and that the recorded footage is treated in accordance with applicable laws and regulations. And it is still just as important that you intervene if you see that someone needs help, even if there are cameras present.

Even if a camera records an event, it can't prevent things from happening.

WHAT DO YOU THINK?

Do you behave differently if you know that a camera is watching you? Is it ok if someone can see everything you're doing, all the time?

Can video surveillance in public places – such as on buses and in schools – result in us assuming less responsibility for our fellow human beings? Are we putting the responsibility in the camera's hands?

Imagine that a student has her wallet stolen in the changing room at school. Should a camera be installed to monitor the changing room? If so, what would the purpose be: to prevent crime or solve cases afterwards? What are the consequences of installing a camera?

TASKS:

Walk around your neighborhood. Note where surveillance cameras have been positioned. Why are the cameras mounted where they are? Do you think they have an effect?

How can footage be abused by those who are carrying out the surveillance?

Regulations governing video surveillance

Everyone who wants to install video surveillance cameras must first inform The Data Inspectorate. All public places, which use video surveillance, must clearly indicate that surveillance is in progress. Concealed surveillance is prohibited. It is prohibited to provide or show recorded footage to third parties without the consent of those who are included in the footage. However the footage may be provided to the police. The recorded footage must be stored in a place to which only authorized personnel have access, and deleted once there are no longer any relevant grounds for retaining it, and no later than seven days after it is recorded.

Camera isn't always best

The United Kingdom is the world's most camera-ridden country, with more than 4.2 million surveillance cameras. A research group from the University of Leicester has studied how surveillance affected the occurrence of crime in selected areas. They found that crime was reduced in only two of the fourteen areas under surveillance. Research suggests that surveillance cameras may, to some extent, contribute to reducing the number of break-ins, robberies and thefts in well-defined and limited areas such as shops and parking lots. There is little evidence to prove that video surveillance in streets and shopping areas has a positive effect in terms of reducing violence in society.

Shutting people out

While the police use CCTV surveillance to prevent and solve crimes, the results of a Norwegian doctoral thesis showed that others are more concerned about excluding unwanted visitors from their areas. Research suggests that camera operators at shopping centers, for example, are not particularly concerned about uncovering crimes or disturbances. Instead, it is more about determining who is wanted in the area. Those who are unwanted are removed – without having done anything wrong.

Cameras everywhere

Oslo is the most camera-ridden city in Norway. In and around Oslo City, Byporten shopping center and Oslo central station there are more than 500 surveillance cameras.

THAT'S LIFE!

More hot dogs on the grill, please!

The young people working at a petrol station in Telemark were repeatedly called by their boss, asking them to put more hot dogs on the grill. How could the boss see how many hot dogs were on the grill if he wasn't at the station himself? The employees suspected that the owner was videoing all or parts of the station, and watching it "live" from his home. An inspection by the summer team of the Norwegian Confederation of Trade Unions (LO) showed that they were right. It is considered a serious infringement to use surveillance cameras in order to monitor your employees in this way. The positioning of the cameras also had to be altered so that they no longer recorded the employees' movements behind the counter.

Source: The Data Inspectorate

Caught on suspicion

A taxi driver had lost his wallet. He was contacted by a store that had found his wallet and driving license on a chair. The driver was allowed to see CCTV footage, which showed that a boy had sat on the chair. The man recognized the boy from the neighborhood, contacted him and accused him of having stolen his wallet. The boy denied it. Even though the footage showed that the boy had sat on the chair where the wallet was found, this isn't proof that he was the one who stole the wallet. The store had no right to show the footage to anyone except the police, and the store was ordered to evaluate its video surveillance procedures.

Source: The Data Inspectorate

Caught on camera in the changing room

Customers at a sporting goods store in Sweden were filmed by a video camera while in the changing room. This secret surveillance was discovered by chance by the local newspaper. The surveillance was said to have gone on for more than a year. According to the store manager, the store needed the cameras due to the high rate of theft. The management of the sports chain stopped using the cameras immediately after this story came to light.

Source: Aftenposten

YOU DECIDE WHO YOU CALL AND WHEN. The telecommunications operator records it. You decide where you use your debit card and what you use it for. The bank records it. You decide which search terms you use in Google. The search engine records it. Over the course of a normal day, you leave many tracks behind you. Many people may be interested in them.

Someone is following your tracks



11. September 2001: terrorists flew into the World Trade Center in New York. The whole Western world quaked in fear of new terrorist attacks. Stricter security controls, including new passports, more wiretapping, the tracing of mobile phones and the monitoring of Internet traffic were introduced to prevent new attacks and other criminal activities.

Use and abuse

The increased fear of terrorism and other serious crime has meant that the boundary for what we are willing to accept in terms of monitoring and surveillance is shifting. Developments in technology mean that this is actually possible. Most people consider using someone's electronic tracks to fight crime as a positive thing, but is it right that we are all more or less treated as suspects in the event that we do something wrong sometime in the future?

Never before has it been possible to gather so much information about each and every one of us. It can also be tempting to use this information for purposes other than what it was collected for. Electronic tracks can be used for purposes we don't like, such as commercial entities that use electronic tracks for marketing and sales.

Good intentions

There are a lot of people, who collect information about you in order to be able to offer good services. For example, you are registered on the public health and school

WHAT DO YOU THINK?

"We are theoretically on the verge of being able to eliminate crime in society, in the sense that every person could be under surveillance at all times. But I am certain that we would have major misgivings about living in such a society, because it probably wouldn't be a good society", says the politician Lars Sponheim. Do you agree with him?

DNA testing of all newborns and a DNA database of all residents may contribute to solving crimes in the future. Do you think it would be a good idea to create this kind of database in Norway? What kind of problems might this cause?

TASK:

Make a list of the organizations that you think have collected information about you, both commercial (such as Internet providers, telecommunications companies, gyms and banks) and public (such as central and local governments, hospitals and schools). Is the list longer than you thought it might be when you started?

databases so that you can be offered good public services. The police and the judicial system need to be able to collect information and check electronic tracks to help investigate crimes and convict criminals, saving lives and maintaining law and order in society.

It is important to establish clear rules on who has the right to collect information about others, how this information is to be used, what it can be used for and how long it can be stored. Information that is collected for one purpose should not automatically be used in other contexts.

More and more of what we do is recorded. Surveillance cameras follow us in an ever increasing number of different places. Someone is watching us and collecting information about us even when we're not doing anything wrong. Some people don't like this idea, even if they know their hands are clean.

Can surveillance always be justified?

The music industry is monitoring file sharing

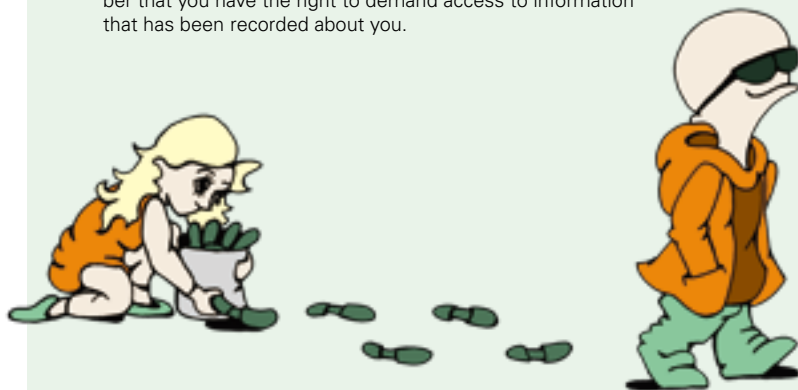
The uploading and downloading of music and movie files without the legal right to make copies is an illegal act. Those who own the rights to the music and movies miss out on substantial sums of money when people illegally download from the Internet instead of paying for the product. This is why in autumn 2006, The Data Inspectorate gave a law firm (that represents the music and movie industry) permission to monitor those areas of the Internet where illegal file sharing occurs. Through this monitoring process, the law firm will gain access to relevant IP addresses. Based on this information, various steps will be evaluated, including reporting suspects to the police.

Everything is recorded

To combat crime the EU has established a Data Retention Directive and the EU countries are in the process of implementing it. The regulatory framework means that information about who people speak with via fixed-line, mobile and IP telephones is to be archived for up to two years, irrespective of the length of a conversation. This also applies to information about who individuals send e-mails to and receive e-mails from, and when they are connected to the Internet. Norway is considering implementing a similar regulatory framework.

You are being recorded

Many people are interested in your personal information and you are recorded on a daily basis. More and more entities are collecting and collating information about you. The police can use the information to uncover crimes, while criminals do it for their own gains. The commercial entities need your information in order to make money. Marketers are interested in obtaining as much information about you as possible. Nothing is free – you pay with your personal information. And remember that you have the right to demand access to information that has been recorded about you.



THEY CAN SEE YOU!

Developments in technology move very quickly and are constantly offering new opportunities:

World of Warcraft

In the online game "World of Warcraft", the operator of the game can "see" whether you are using a code-breaking website while you play. If you cheat, they can expel you from the game.

Tailored advertisements

Gmail uses a program that scans the e-mails you write and looks for words that identify something that you're interested in. Google then tailors its advertisements accordingly.

Electronic tickets

These enable the transportation company to figure out where you've been, and when. The information is saved, and you can easily check where you've been recently by using the company's website.

Fingerprints and DNA

Fingerprints, iris scanning and other biometric measurements are technologies that are beginning used in ever-increasing circles. There are plans afoot to include fingerprints in new Norwegian passports. Some people want to create a national database of people's DNA. Such a database will make it easier to catch criminals, but the information can also be abused.

Protecting personal data means that there are rules for how other people can use information about you. We hope that you now have a better basis for deciding what information you want to give out, and who you want to give it to.

Although there will be situations where you don't always have complete control, we hope that you nevertheless feel a bit more secure. Because in most situations it's really **YOU WHO DECIDES!**

Interested in finding out more?

At www.dubestemmer.no you'll find more information about protecting your personal data and the legislation involved. You'll also find links to other useful information and other groups that provide information about this area. You can also contact The Data Inspectorate by telephone on **+47 22 39 69 00** or by e-mail at postkasse@datatilsynet.no.





www.dubestemmer.no