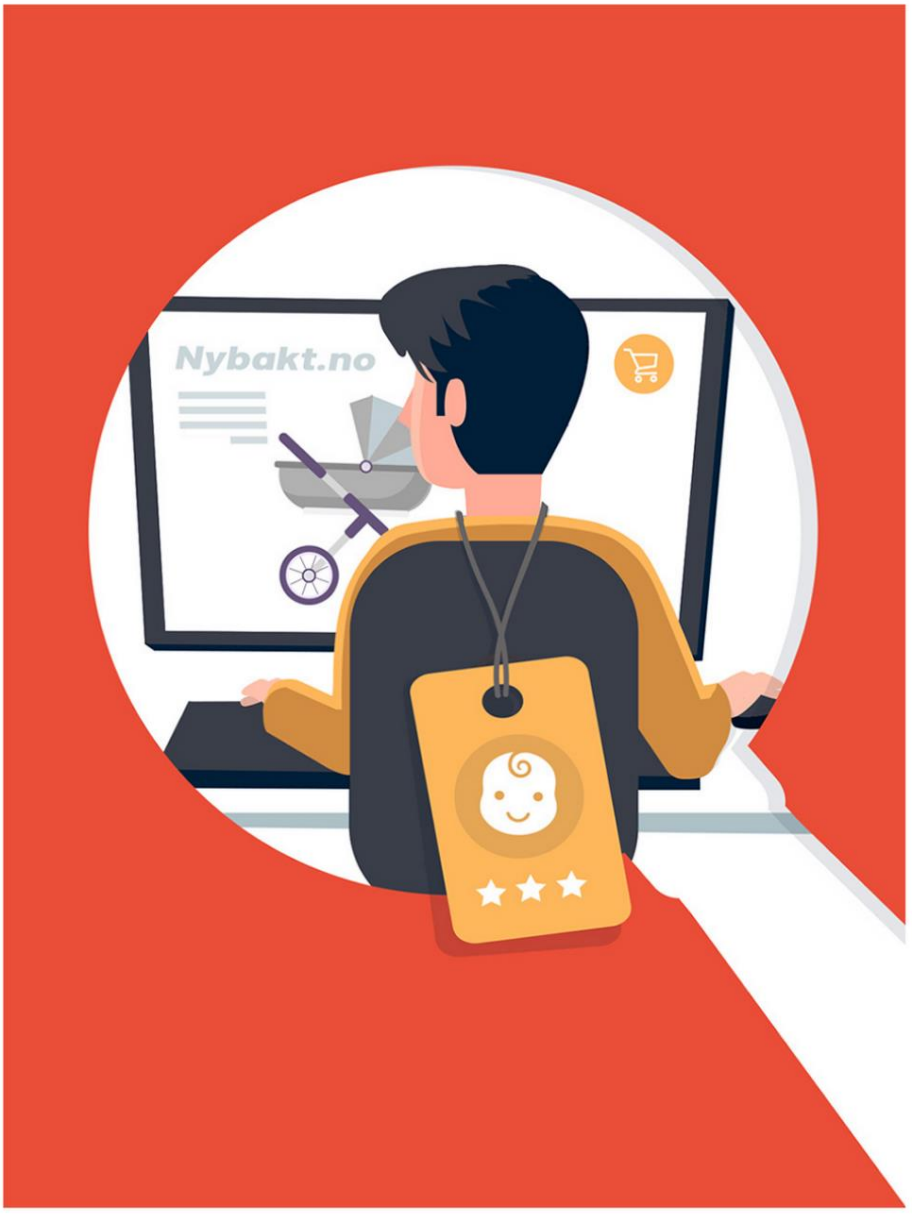


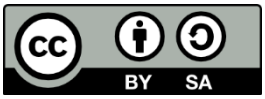
COMMERSIAL TRACKING IN THE PUBLIC SECTOR

Teknologirådet

COMMERCIAL TRACKING IN THE PUBLIC SECTOR

ISBN 978-82-8400-011-4

Published: Oslo, March 2021
Cover illustration: Birgitte Blandhoel
Published electronically at: www.teknologiradet.no



FOREWORD

"If something is free, you're not the customer, you are the product"

This quote from Bruce Schneier describes what is referred to as the surveillance economy – where digital services are offered for free in exchange for the collection of vast volumes of data about users. This data is subsequently used in the advertising industry in order to influence our behaviour through targeted advertising.

In this report, we aim to highlight how the surveillance economy and online tracking have entered the public sector. By using freely available tools from the tech giants, public sector websites invite commercial actors into the most innermost spheres of our lives.

This development is problematic, as public sector services are sensitive and private and there are no alternative service providers. The public sector should therefore take particular responsibility not to share data about us with commercial players.

The Norwegian Board of Technology is an independent body that advises the Norwegian Parliament and the government on new technology and promotes an open, public debate. We hope that this report will contribute to an enlightening discussion of how the public sector can take the privacy of citizens seriously – including when services are digitised.

Tore Tennøe

Director, the Norwegian Board of Technology

CONTENTS

SUMMARY

The public sector currently contributes to data about citizens being collected and shared with the largest players in the surveillance economy. This is a democratic issue, as it is not possible to opt out of such surveillance and a competitive policy issue because it strengthens digital monopolies.

THE DIGITAL ECONOMY IS BASED ON SURVEILLANCE

A number of actors keep track of what we do when we use the internet. Information about the websites we visit, who we follow on social media or which films we watch are all examples of information that is valuable to the advertising industry. This has led to a trend in which many digital services are available free of charge in exchange for the collection of vast volumes of data about users. This is, for example, the basis for services provided by Google and Facebook, as well as a wide range of apps and games.

Because it is possible to track users across various websites and devices, the companies in the advertising industry can create digital profiles. By analysing online behaviours, movement patterns and habits, these digital profiles can become highly detailed and can form a complex and personal picture of users. The profiles may, for example, include information about personality types, personal relationships and sexual preferences, as well as gender and age, place of residence, place of work, language and interests.

MARKET DOMINATED BY GIANTS

The digital advertising market is vast and complex and involves many different players. The tech giants, such as Google and Facebook, dominate the market and it is estimated that these two companies receive more than half of the money spent on digital marketing worldwide.

The fact that these companies already possess vast volumes of data makes it difficult for competitors to become established or challenge their positions. Google and Facebook are also involved in different ways at the same time – they both buy and sell ads and ad space.

VARIOUS TOOLS TRACK NEARLY ALL ONLINE ACTIVITIES

There are many different methods and techniques available for tracking on websites.

Cookies, web beacons and **digital fingerprints** are all techniques that allow your browser to collect and share information about your online activities. If a company uses tracking on many different websites, it is also possible to follow a user across these sites. As these techniques are so prevalent, this results in some companies amassing enormous volumes of data about each individual's online activities.

Many web browsers allow you to block the use of cookies, but it is harder both to detect and block the use of web beacons.

Recording website visits and **keylogging** are two other techniques that can be used to track activities. Recording website visits can be compared to someone standing behind your back, keeping an eye on every click you make, move the mouse or scroll. This can then be replayed after your visit to the website. Keylogging means that any text entered in forms, chats or anywhere else is recorded – including before you have clicked send or save.

Both of these techniques are associated with a high risk of sensitive data being collected and shared with unauthorised parties, for example if you submit credit card information, health information or contact information using a form.

Google and **Facebook** have their own tracking tools that are very widespread. Google Analytics is a free web analytics service that tracks and reports website trafficand is estimated to be used on over half of all websites worldwide. Detailed information about the use of the website is normally shared with Google.

Facebook Pixel is used to gain an insight into how users react to ads that have been published through Facebook. This means that it is possible to follow a user's activity when they click on a Facebook ad or more generally on websites where Pixel is installed. Here, activities can be linked to named users if the users are logged in to Facebook.

In combination, these tools mean that virtually all online activity is tracked, stored and shared with actors in the advertising industry. Since Google and Facebook already possess vast volumes of data and own some of the most widespread tools, this contributes to further strengthening their positions in the market.

COMMERCIAL TRACKING IN THE PUBLIC SECTOR

Public sector digitisation is fully under way. The principle of digital first choice means that communication between citizens and the authorities will take place predominantly online.

In this report, the Norwegian Board of Technology has examined 41 public sector websites using the tool Blacklight. Blacklight examines which tracking technologies are active on the websites and which parties receive information about user activity. We have also reviewed the privacy policies of the websites to look at how they describe the tracking that takes place on the websites.

A total of 36 of the websites use Google Analytics and several also use other tools from Google. Hotjar, a tool used to record website visits, is also in widespread use. Facebook Pixel is less common and was used by only four of the websites.

A democratic issue

Of the 41 websites, 38 share data with commercial players. Citizens cannot opt out of public services and these services may involve the sharing of data linked to health, family life and personal finances.

Information such as a citizen applying for parental leave or a place in kindergarten is attractive information on the digital advertising exchanges and may be used to sell ads for prams or new winter shoes. It is therefore concerning to find that the Norwegian Labour and Welfare Administration (NAV) uses three analytics tools from Google and states that the website will no longer work as intended if you refuse cookies.

Another example is the Norwegian Directorate for Children, Youth and Family Affairs (Bufdir), which is transparent about the fact that they track individuals who have visited their websites relating to foster homes in order to subsequently show them Facebook ads about becoming foster parents.

There are often no alternative service providers. The public sector should therefore take particularly great responsibility when it comes to security and the protection of personal data.

Difficult to understand

Many companies give the impression that users are in control of how data is collected and used. However, in many cases, this is a purely superficial process as the alternative to not consenting to tracking is to not use the website at all.

Privacy policies are also difficult to understand. Unless you have knowledge and understanding of the tracking technology used, it is virtually impossible to understand what actually happens. Many privacy policies are also inadequate or incomprehensible.

Strengthens already dominant players

In addition to using the information to influence users' behaviour through advertising, widespread tracking also helps increase market dominance, especially on the part of Google and Facebook. The significant access these companies have to data is a major reason for this dominance.

There are ongoing policy measures globally and in Norway at present with the aim of avoiding such market dominance, especially in the digital economy. The fact that the public sector, including the Norwegian Consumer Authority, the

Research Council of Norway and Innovation Norway, contributes to this by using free tools from the tech giants is therefore problematic.

WHAT CAN BE DONE?

The public sector should take the lead and assume particular responsibility for providing citizens with strong digital services – without allowing commercial players to come along for the ride. There are three measures that can help make the surveillance economy a less attractive business model.

Minimising data collection and providing better information

Several of the websites justify tracking with the importance of user-friendliness and therefore consider this to be more important than users' privacy. We believe that user-friendliness can be achieved in different ways and without the involvement of commercial players. The public sector should choose solutions and tools that comply with the principles of privacy and should therefore collect minimal data, and only for very specific purposes only.

If data is collected at all, it is important to be able to explain the purpose of the tracking in a clear and simple manner.

Pay using money, not data

Google does not offer its analytics tools for free out of the kindness of its heart, but because they see the value of the data collected using the tool. The public sector should make an active choice not to participate in the surveillance economy and should pay for the tools they use with money – not citizens' data.

Consider a ban on microtargeting

One of the reasons data is collected is for use in the microtargeting of ads. There are already many examples of how such personalisation techniques have influenced democracies and social structures around the world. Microtargeting in advertising should therefore be banned, which would also ensure more equal competitive terms, as personal data would become less important.

THE SURVEILLANCE ECONOMY

The business model in the digital economy is largely based on the monitoring of users. Information about what we do, our habits and our interests is used to present us with targeted ads.

There are a number of companies that keep track of what we do when we use a website. Information about the websites we visit, who we follow on social media or which films we watch are all examples of information that is valuable to the advertising industry. The more they know, the more precisely ads can be targeted. Data about users therefore becomes a valuable commodity in the advertising market.

THE TECHNOLOGY THAT DRIVES DEVELOPMENTS

There are four developments that have contributed to the surveillance economy becoming so widespread:[1]

- **The Internet of Things:** An increasing number of objects around us are being equipped with sensors and connected to the internet. Additionally, more and more technology is being carried directly on the

[1] The Norwegian Board of Technology (2016)

body through the development of smartwatches, pulse belts and other wearable technology.

- **Data and metadata:** All computers produce vast quantities of data. As society around us becomes digitised, our lives are also becoming increasingly documented. Metadata is also becoming increasingly important – the data that describes the circumstances surrounding our online activities.
- **Cheap storage:** Computers are increasingly being equipped with larger and more affordable storage. This means that more and more data can be stored.
- **New correlations shown by big data, affordable computing and machine learning:** The development of artificial intelligence makes it possible to continuously identify new correlations in big datasets: Nearly all types of data can be useful and can be analysed in ways that were previously not thought possible.

SURVEILLANCE AS A BUSINESS MODEL

In the beginning, there was little commercial interest on the internet. Towards the end of the 1990s, when companies eventually started to establish a presence online, they started looking for ways to make money. Since users had become accustomed to services being free, user payments were ruled out. There was also no established infrastructure in place for micropayments. Advertising, for example in the form of banners, was launched as an alternative.

However, in order to attract advertisers, the online ads had to offer something you could not get elsewhere.[2] Since it was already possible to analyse the behaviour of users online, this was used to offer targeted advertising.[3]

Google's development is an excellent example of this. When the founders, Larry Page and Sergey Brin, launched their search engine in 1998, they wanted to avoid linking search results and advertising. The search results should not be

[2] Zuckerman, Ethan (2014)
[3] See also the summary of developments here (in Norwegian) https://www.digi.no/artikler/debatt-nordmenn-til-salgs-overvaknings-okonomien-er-fortsatt-ute-av-kontroll/503821

influenced by commercial interests, but should be transparent and based on a ranking scheme inspired by academic referencing practices.[4] At first, therefore, they made money from the sale of licenses, including to Yahoo!.

Nevertheless, the business model changed over time, especially after the dot-com bubble burst and investors disappeared after 10 March 2000.[5] In October 2000, Google launched the AdWords tool, allowing advertisers to buy space at the top of search results. Based on search terms and vast volumes of data about users' online history, Google was able to offer targeted advertising where customers paid for clicks rather than impressions. This led to the company becoming a dominant player in the advertising market and an outstanding commercial success, even though users can still use the search engine without it costing them any money.

This has gradually become the dominant model for digital services: the majority of services are offered for free in exchange for the collection of enormous volumes of data about users in order to grab their attention and sell advertising. Today, this is the basis for popular services from Facebook and Google, as well as a number of popular apps and games.

DIGITAL PROFILES

Because it is possible to track users across various websites and devices, the companies in the advertising industry have the opportunity to create digital profiles on users. The information that is collected is put together from multiple sources. One such type of information is information about the content you interact with: which websites and apps you use, who you are friends with on social media and what you search for. Metadata is also collected – for example what devices you use, your geographical location or the times during the day which you are most often online. Based on this information, digital profiles may also include *derived information*. This means that companies such as Facebook make assumptions about a number of things based on the information they have access to, for example ethnicity, interests and financial circumstances.

By analysing our online behaviours, movement patterns and habits, these digital profiles can become highly detailed and can form a complex and personal

[4] Brin, Sergey and Lawrence Page (1998)
[5] Foroohar, Rana (2019)

picture of us as individuals. The profiles may, for example, include information about personality types, personal relationships and sexual preferences, as well as gender, age and interests, place of residence, place of work and language.

These profiles form the basis for targeted advertising online. Based on our interests, preferences and finances, advertisers are able to personalise their message and even predict our future needs.[6] The goal is to attract and retain our attention and, over time, make us to do things such as react to content and click on ads. On YouTube, 70 per cent of the content seen by users has been selected based on the recommendation algorithms in the video platform.[7] Accordingly, the platforms themselves largely control the content users see and react to.

There is growing awareness that information about online activity is used for targeted advertising. The fact that the information is stored in complex digital profiles comes as more of a surprise to many.[8] When targeting is done in a clear and transparent way, such as through recommendations on Netflix or Spotify, many people consider it to be a positive thing. However, data is also widely used to personalise search results, advertisements and services in less visible ways.

A recent survey from the USA shows that no less than 81 per cent of respondents are concerned that the data that is collected about them is being used to create complex digital consumer profiles.[9]

BUYING AND SELLING ON ADVERTISING EXCHANGES

The digital advertising market is vast and complex and involves many different players. On a very general level, the players can be broken down into four categories:[10]

- **Publishers** sell access to interfaces where various advertisers can buy ad space. Examples of publishers include online newspapers, blogs, mobile games and social media.

[6] Christl, Wolfie (2017)
[7] Solsmann (2018)
[8] Which? (2018)
[9] Consumer Reports (2020)
[10] The Norwegian Consumer Council (2020)

- **Advertisers** include all companies, businesses and organisations that want to reach new and existing customers through digital advertising.
- **Third-party providers** are a large group of different companies that sell services to publishers, marketers or other providers. These companies may be analytics companies or data brokers.
- **The major platforms,** such as Facebook and Google, have assumed dominant positions, amongst other things because they are sitting on vast amounts of data. They often hold multiple roles at the same time and control several levels of the market.

When you visit a publisher's website, an auction is launched in which various advertisers compete to buy advertising space. Within milliseconds, the user's digital profile is presented to potential advertisers. The advertiser that is willing to pay the most wins and this will be the one whose advertisements the user is presented with on the website. The entirety of this fully automated process takes place in the time it takes for the website to load.

The price paid for each advertisement is low. However, there are certain types of data that can result in increased value.[11] Major life events such as marriage, moving house or pregnancy often lead to changes in purchasing patterns and this provides advertisers with an opportunity to make money. Information about events such as these will often mean that you become a much more attractive target in the advertising market. Health information, particularly relating to the use of pharmaceuticals, is most attractive and can almost double the price advertisers are willing to pay.

MARKET DOMINATED BY GOOGLE AND FACEBOOK

It is estimated that Google and Facebook combined receive more than half the money spend on digital marketing worldwide.[12] In Norway, the advertising market is estimated to be around NOK 20 billion, of which Facebook and Google have a share of six billion.[13] This share is significantly higher in many countries. In the USA, it has been estimated that the two companies received nearly 70 per cent of digital advertising revenue in 2019 and in the UK their share has been estimated to be no less than 80 per cent. Google and Facebook

[11] Steel, Emely (2013)
[12] eMarketer (2020)
[13] Ekeberg (2019)

are the largest companies within the surveillance economy and have been ranked as the fifth and sixth most valuable companies in the world respectively.[14]

Google

Google started out as a web search engine but has now also become a dominant player in many areas of the digital economy. The Chrome web browser is the most widely used web browser in the world and Google Maps accounts for 80 per cent of digital map usage.[15] Together with services such as YouTube, Google Translate, Gmail, Google Workplace, the home assistants Home and Nest and the Android operating system, the company has created its very own product universe on the basis of data collection.

Many people may be less familiar with Google Analytics, a free web analytics service that tracks and reports website traffic. This is the most widespread tool on a global level and it is estimated that more than half of all websites worldwide use Google Analytics.[16] By installing a small code on the website, Google Analytics can be used to monitor activity on your own website, such as where users originate from, which pages they visit, etc. Website owners thereby get a free tool for traffic analytics, while Google gets access to the data that is collected.

Google's access to data through all its services allows it to dictate many of the mechanisms in the advertising market. Google owns DoubleClick, the largest advertising exchange, while also selling and buying both ads and ad space. In other words, they hold the role of publisher, marketer and third-party provider at the same time.

Google was one of the first companies to produce targeted advertising based on their access to personal data about users. And this is still where the company's main revenue is found. In 2019, the company made nearly USD 135 billion from advertising alone.[17]

Facebook

With nearly 3 billion users, Facebook is the largest social network in the world. The company also owns the highly popular services Instagram, Messenger and WhatsApp. These four services were the most frequently downloaded apps in

[14] Statista (2020)
[15] Subcommittee on antitrust, commercial and administrative law of the committee on the judiciary (2020)
[16] W3Techs (2020)
[17] Véliz, Carissa (2020)

the 2010s.[18] Facebook's business model is based on the collection of data about users and non-users by following their online activities both on and off Facebook. They then sell access to the data via their advertising tools. Based on this business model, Facebook is predominantly an advertising platform that collects data about its users through user participation in groups and networks.

In recent years, Facebook has continuously developed its products and has retained a dominant market position with far more users than any of its competitors within social media. In fact, several of Facebook's main competitors are owned by the company itself.

This dominant market position makes Facebook an attractive advertising platform. Another advantage is the possibility to target ads to actual, named individuals and not just digital user profiles.[19] Such individual targeting can be performed by a company uploading its customer list to Facebook, linking these names to the customers' Facebook profiles and targeting ads directly at these customers.

The high number of users provides advertisers with a large audience and they also gain access to complex tools for the targeting, testing and improvement of their ads. One of these tools is Facebook Pixel. When someone clicks on an ad, Pixel makes it possible to monitor what the user does on the site – such as whether or not they make a purchase.[20]

One of the most popular tools available via Pixel is the ability to target ads at users who have previously visited your website. Rather than using target groups based on age, gender or place of residence, you can present ads to those who have already shown an interest in what you are selling.

Facebook possesses a treasure trove of data about us, regardless of whether or not we use their services. This is data that has been collected through user profiles, customer lists uploaded to the advertising tools or data collected through Pixel on countless websites. Facebook also has a somewhat murky reputation when it comes to how data is shared and processed, in part following the Cambridge Analytica case in 2016.[21]

[18] Shead (2019)
[19] Subcommittee on antitrust, commercial and administrative law of the committee on the judiciary (2020)
[20] Facebook (undated)
[21] Wired (undated)

HOW WE ARE TRACKED

The number of ways in which we can be tracked online is constantly growing. Cookies have been joined by web beacons, keylogging and video – and not least the analytics tools from Facebook and Google.

There are several different tools and methods available for tracking online activity. Additionally, both Facebook and Google have their own services that collect data across a vast number of websites.

Online tracking has traditionally been performed using cookies. Increased awareness of such tracking has, among other things, resulted in several web browsers, such as Firefox, Edge and Safari, now blocking third-party cookies in order to protect the privacy of users. Information about users is such a key aspect of the internet economy that other tracking technologies are now used to a much greater extent than before in order to circumvent these blocks.

An increasing amount of our online activities now take place via mobile devices and apps. Dedicated tracking technologies and techniques are also being developed here in order to identify users. For example, ad or device IDs are now common in the digital advertising industry. By assigning a unique number to each user or device, it is possible to keep an eye on what the user does across services

and devices.[22] This means that it is also possible to develop complex profiles linked to each ID number.

In this report, we will focus on tracking on websites and describe the predominant tracking techniques used in web browsers. The most important of these are addressed below.

COOKIES

Cookies have traditionally been the most widespread type of online tracking. When you visit a website, a small snippet of code is stored in your web browser, allowing you to be recognised on subsequent visits. The file ensures that the website owner receives information about what users do when visiting the website.

There are several different types of cookies. First-party cookies are used when the owner of a website decides to use cookies to obtain information about what visitors do, for example for statistical purposes. This also makes it possible to store login information or language settings for subsequent visits.

Third-party cookies are placed on a website by parties other than the party that owns the website and such companies often place cookies on many different websites. This makes it possible to identify and map users' activities across all of these websites. This is common within the advertising industry and makes it possible to personalise advertising based on individual online activity.

WEB BEACONS

Web beacons are invisible image files that are placed on websites, either in combination with or instead of cookies.

Websites that contain images always store these images on a server. When you visit a website, your web browser will download these images to show them to you. The same happens when a website uses web beacons: the web beacon is

[22] The Norwegian Consumer Council (2020)

downloaded by the web browser. When the image is downloaded, a number of data points are sent back to the owner of the website, including IP address, technical settings and what you do on the website.[23]

Web beacons are used to collect information about user activities on websites in the same way as cookies. Even if a web browser does not consent to cookies, web beacons will continue to collect data about user activity.

Web beacons are often used to collect information for personalisation of advertisements and are also commonly used in newsletters in order to collect information and analyse user behaviour, for example to see how many users click on links contained in a newsletter.[24]

DIGITAL FINGERPRINTS

A digital fingerprint is a method for identifying users that is based on the compilation of various pieces of information and the technical device used.

In order for a website to display correctly, the web browser shares a wealth of information with the website owner – such as screen resolution, language settings and operating system. When these details are collated, the result is a digital fingerprint that makes it possible to identify the user. In this way, websites can recognise you every time you visit.

This technique was developed for security purposes and is still used for this purpose in order to expose software piracy, identity theft or credit card fraud.[25] Digital fingerprints are difficult to identify and delete, as the technique is not based on the installation of software (such as cookies, for example) or the registration of the IP address.

Digital fingerprints are used in particular by third-party players in the advertising industry, for example data brokers. Because these players are active in large parts of the internet, users' activity can also be followed across multiple websites.

[23] The Verge (2019)
[24] Whatagraph (2019)
[25] Briz, Nock (2018)

This technique was developed around 2010 but has not been particularly widespread. In 2019, the technique was used on around 3.5 per cent of the most popular websites. Nevertheless, this represented an increase from around 1.6 per cent in 2016. The technique is also used in a number of apps.[26] Because cookies are now blocked in many web browsers, alternative methods are becoming increasingly popular.

KEYLOGGING

Keylogging means that a website or third party records what you type into a form, even before you click "send" or "save". It can also include the collection of metadata – how quickly you type or how hard you press the keys.[27]

Keylogging can be used in several ways. One example that many people are familiar with is when you start typing text into a search field and text suggestions appear. It can also be used in security work, for example to detect unauthorised activity in a server. Typing metadata can be useful in recognising individuals. In this case, it is not *what* you type but *how* you type that is analysed.[28]

Because most digital services include text elements, keylogging may inadvertently reveal sensitive information. This could include credit card information, passwords or personal identification numbers. If you enter this information into a form and keylogging is used, this information could subsequently be made available to parties other than the intended party.

This information can subsequently be used both in targeted advertising and also in various types of fraud.

RECORDING OF WEBSITE VISITS

The recording of website visits means that an entire visit to a website is recorded and stored as a video recording.

[26] Chen, Brian X. (2019)
[27] Kaspersky (undated)
[28] Baisotti, Valentina (2019)

This includes all minor and major activity, such as the movements you make with the cursor, the pages you visit and when you scroll up and down. You could compare this technology to someone standing behind you, keeping an eye on all of your movements.

When you can watch recordings of how users navigate a site, you get an insight into whether it is difficult to navigate or perform the tasks the users came to the website to perform. It can therefore be a useful tool for improving the user-friendliness of websites. However, it also poses privacy challenges. Analysing such recordings does mean that information that has been typed in forms could become visible, for example names, addresses, passwords or medical information.

Hotjar is a popular tool for the recording of website visits. Of the 41 websites examined by the Norwegian Board of Technology, 14 websites shared information with Hotjar.

GOOGLE ANALYTICS

Google Analytics is a free web analytics service that tracks and reports website traffic. It is extremely widespread and estimated to be used by more than half of all websites.[29]

A small snippet of code is installed on the website in order to use the tool. This code snippet records everything users do. The website owner therefore gains access to information about e.g. where the user is located, which pages they visit, how they found the website, etc. The same information is normally also shared with Google.[30]

Data from Google Analytics can be linked to data from Google's advertising services, making it possible to monitor how users interact with ads, as well as the website itself. This facilitates targeted advertising. The *Remarketing Audiences* tool, for example, means that it is possible to target advertising to users that have previously visited a website in order to entice them to return.

[29] W3Techs (2020)
[30] Google (undated)

Google Tag Manager is another common tool. This is used to configure and keep track of various activities on a website. As an example, "tags" can be configured to track specific activities, such as completed purchases in the online store, downloading of a document or completion of a form.[31]

As described in the previous chapter, Google performs various different roles in the advertising market. The many services run by Google and the large number of websites that use Google Analytics means that Google has access to information about a very large proportion of global online activity.

FACEBOOK PIXEL

Facebook Pixel is a free tool from Facebook, which analyses interactions with ads on Facebook's advertising platform and visits to websites on which Pixel has been installed.

In the same way as Google Analytics, Pixel is used by installing a small snippet of code on a website. This snippet of code records user activity.

Facebook Pixel is linked to Facebook's advertising services. This provides insight into how ads perform on Facebook, as it is possible to monitor users' actions when they click on an ad. Whether or not users end up buying a product and any other products they look at are examples of information obtained using Pixel. This also facilitates targeted advertising based on activity on pages and apps outside of Facebook.

Pixel also checks whether website visitors are logged in to Facebook, Instagram or WhatsApp. If they are, information about the website activity will be linked to the Facebook user in question. This means that Facebook is able to track users on many different websites outside of its own platforms. Because many people are logged in to Facebook both on their mobile and on their PC, they can also be tracked across devices. Facebook Pixel also collects information about individuals who do not have Facebook accounts. This information cannot be linked to a named person, but data is still collected and used to further develop a digital profile.

[31] Fedorovicius, Julius (2020)

PRIVACY CHALLENGES

The use of cookies, web beacons and digital fingerprints is generally fairly similar. The techniques are used to collect information about how we use and move between different websites. Many providers in the advertising industry are widely represented online, allowing them to track us across many different websites.

While we have gradually developed relatively good options for blocking cookies, it is now becoming much more common to use web beacons and digital fingerprints and these are much harder both to identify and delete.

Keylogging and the recording of website visits are slightly different technologies. One privacy challenge associated with the recording of website visits is that sensitive data could be recorded and stored.[32] This could include identifiable data such as name and address, as well as health information or credit card information. Keylogging is associated with similar challenges, but here there is also a risk that a website might collect information that has been typed into a form but never submitted. It could therefore be argued that this technique can collect information about what we think, not only what we actually do.

The comprehensive use of tools from Google and Facebook is problematic in and of itself. It means that these two companies have an overview of large parts of current internet usage. They are therefore also able to track users across various websites and devices.

Even though each little snippet of information does not say much about each user, a larger compilation of online usage will provide a detailed and personal picture of habits, preferences, networks and activities.

[32] Kassner, Michael (2017)

COMMERCIAL TRACKING IN THE PUBLIC SECTOR

The public sector performs a number of tasks and services that citizens depend on and do not have the opportunity to opt out of. This makes it even more important to ensure that privacy is safeguarded.

Public sector digitisation is fully under way. The principle of digital first choice means that communication between citizens and the authorities will predominantly be digital.[33]

Public services often deal with citizens with regard to sensitive matters and such services may involve the sharing of personal data linked to health, family life or personal finances. There are often no alternative service providers. The public sector should therefore take particular responsibility when it comes to security and the protection of personal data as services are digitised. This involves ensuring that no more data is collected than is absolutely necessary.

In 2016, the Norwegian Consumer Council examined the websites of Norwegian municipalities, with disappointing results.[34] Many municipalities shared information about their users with a large number of third parties, many of which

[33] The Norwegian Digitalisation Agency (undated)
[34] The Norwegian Consumer Council (2016a)

were linked to the advertising industry. Many of the websites also did not have privacy policies.

IS THIS LAWFUL?

WEB TRAFFIC ANALYTICS

The use of services such as Google Analytics may involve the collection and analysis of personal data. IP addresses, for example, are defined as personal data, as they can be traced back to a specific computer and user.[35]

The lawfulness of Google Analytics and similar tools was assessed by the Norwegian Data Protection Authority in 2012. The Authority conducted audits at the Norwegian State Educational Loan Fund and the Norwegian Tax Administration and examined which data was collected and how the data was processed.[36] After obtaining documentation from Google, which described how IP addresses were processed and stored, the use of Google Analytics was approved, provided that parts of the IP address were masked before the information was stored on Google's servers.[37]

The vast majority of the websites examined by the Norwegian Board of Technology state in their privacy policies that they comply with the guidelines from the Norwegian Data Protection Authority and mask IP addresses. Nevertheless, there are some that do not address this matter, such as the municipalities of Tromsø and Bergen, the Norwegian Directorate for Civil Protection, the Norwegian State Housing Bank and the Norwegian Institute of Public Health. It is therefore impossible to know whether or not these websites do ensure such masking.

USE OF COOKIES AND CONSENT

The use of cookies is governed by the Norwegian Electronic Communications Act, which is managed by the Norwegian Communications Authority (Nkom).[38] The act stipulates that users must receive information about and give active

[35] The Norwegian Data Protection Authority (2018)
[36] Jørgenrud, Marius (2012)
[37] Jørgenrud, Marius (2013)
[38] The Norwegian Communications Authority (2020)

consent for the use.[39] This means that it must be clear which cookies are used, which data is processed, what the data will be used for and who the data is processed by.

The data protection authorities in both the UK[40] and Belgium[41] are currently dealing with cases relating to the digital advertising industry and online tracking and consent is one of the elements being considered. In Belgium, a statement is expected to be published at the start of 2021. The authorities are also getting involved in Norway. In January 2021, the Norwegian Data Protection Authority notified the Grindr dating app that it would be issued a fine of NOK 100 million.[42] The Authority pointed to the fact that Grindr had shared users' personal data with third parties without valid consent.

TRANSFER OF DATA

During the summer of 2020, Privacy Shield, the agreement that governs the transfer of data between the EU and the USA, was found to be invalid.[43] Because US intelligence legislation makes it possible to access data held by private companies, the European Court of Justice found that data from European users does not have adequate protection in the USA.[44]

In the advertising industry, many of the dominant players are American and the data collected is therefore mainly sent for storage on American servers.[45] Such transfer is now unlawful, which therefore affects many Norwegian businesses that make use of e.g. Google Analytics. The use of Google Analytics and Facebook Connect has now been put in the spotlight by the privacy activist Max Schrems and his organisation, NYOB.[46] More than 100 companies that use these tools, including three Norwegian companies, have been reported to the European data protection authorities because they are continuing to transfer data to the USA without a valid agreement.

[39] The Norwegian Communications Authority (2020)
[40] McDougall, Simon (2020)
[41] Lomas, Natasha (2020)
[42] The Norwegian Data Protection Authority (2021)
[43] Court of Justice of the European Union (2020)
[44] The Norwegian Data Protection Authority (2020)
[45] Drange, Jan Morgen and Vebjørn Søndersrød (2020)
[46] NOYB (2020)

WHY IS THIS PROBLEMATIC?

A DEMOCRATIC CHALLENGE

Citizens' interactions with the authorities include some of the most private aspects of our lives. Which public sector websites we visit, which services we use and which agencies we communicate with can generate a great deal of information about our lives that we would not want others to have access to. Increased digitisation and the digital first choice now mean that citizens have to interact extensively with public agencies and services online.

The public sector relies on citizens' trust in order to implement digitisation projects. A key element of gaining and retaining trust from citizens involves ensuring that information about the use of public services is not shared with unauthorised parties. In order to maintain trust between citizens and the state, it should go without saying that public sector websites must be a space that is completely free from commercial tracking.

When it is also the case that certain life events make users more attractive to advertisers, there are even greater reasons to avoid sharing data from the use of public services. Information such as a citizen applying for parental leave or a childcare place can quickly be used to sell ads for prams or new winter shoes.

HARD TO UNDERSTAND WHAT IS HAPPENING

Many websites give the impression that users are in control of how data is collected and used. The many pop-up windows asking us to consent to the use of cookies are all examples of this. However, this is often a purely superficial process, as the alternative to consenting to the use of cookies is to not use the website at all. The Norwegian Consumer Council has previously pointed out how speculative website design manipulates users into consenting to more surveillance than they would otherwise have done, for example by consenting to the collection and analysis of data concerning web usage.[47]

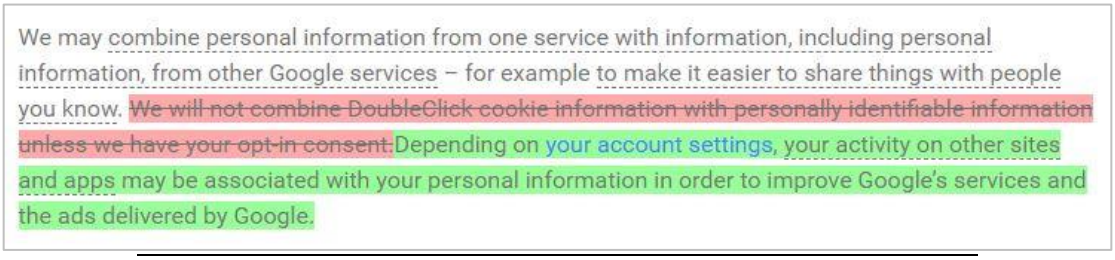
Privacy policies are also often difficult to understand. The choice of words, formulations and the amount of information makes it virtually impossible for a user to understand what they are consenting to. This relates both to the collection of data specifically but also to how data is shared and resold within the vast

[47] The Norwegian Consumer Council (2018)

ecosystem linked to digital advertising.[48] The government has previously noted these challenges, as well as the fact that such challenges lead to users not reading the complete privacy policies or consenting to agreements that they have not understood.[49]

Privacy policies often include a clause stipulating that the terms may be updated at any time and that the user is responsible for remaining informed of any such changes. As a result, this could lead to many users not noticing any fundamental changes in how data is collected and used.

In 2016, Google changed a small sentence in its privacy policy. However, this led to major changes in how Google links data from various services. Previously, information from the DoubleClick advertising exchange had not been linked to identifiable data from Google accounts. In 2016, the change meant that data from user accounts could be linked to data collected from cookies.



The image shows the changes to Google's privacy policy in June 2016.[50]

Several of the public sector websites examined by the Norwegian Board of Technology state in their privacy policies that they use the opportunities available to anonymise data (e.g. masking of IP addresses) and that they share minimal amounts of data. Nevertheless, it is still difficult to work out specifically how data is used and shared with others and for which purpose. Privacy policies are difficult to read and, unless you have knowledge and understanding of the tracking technology used, it is difficult to understand what will actually happen. Many of the privacy policies are also inadequate or completely lacking in descriptions of how tracking takes place on the website.

There are several tools that can be used to block cookies from being installed and used when visiting a website. However, several of the websites warn against this as it can result in the website not working as intended. In turn, this makes

[48] Kemp, Katharine (2019)
[49] Report to the Storting no. 27 (2015–2016)
[50] Retrieved from https://www.google.com/policies/privacy/archive/20160325-20160628/

it even more difficult for users to take their own steps to prevent the collection of data.

STRENGTHENS ALREADY DOMINANT PLAYERS

In addition to using the information to influence our behaviour through advertising, widespread use of such tools also helps increase market dominance, especially on the part of Google and Facebook.

The significant access they have to data is a major reason for this dominance. The two companies collect vast amounts of data through their own services, as well as the data they collect through third parties. And the more people that use them, the more data they amass and the more attractive they become to new advertising customers.

The dominant position of the companies means that these companies earn much more than would be the case if there was greater competition, which was described, among other things, in a detailed report issued by the UK competition authority.[51]

When a small number of companies acquire such monopoly-like positions, it can also hinder more general innovation. This may be of particular relevance to the digital economy, in which data has become the raw material for many types of services, not only marketing. When data largely is gathered by those already holding strong market positions, it becomes difficult for newcomers to establish themselves, even with completely different services, because they do not gain access to the data required to develop new services and concepts.[52]

This market situation is the reason why the competition authorities in e.g. the UK, the USA and the EU are now actively working to limit the dominance of the major players. In December 2020, it became clear that the US competition authorities would be bringing legal proceedings against Facebook[53] and the authorities in Texas and nine other states are now also bringing legal proceedings against Google.[54] Both of these cases relate to the companies' misuse of market power.

[51] The Competition and Markets Authority (2020)
[52]The European Consumer Organisation (2019)
[53] Federal Trade Commission (2020)
[54] Paul, Kari (2020)

The Norwegian authorities also have a stated goal of limiting the market dominance of the tech giants. In the allocation letter from the Norwegian Ministry of Trade and Industry to the Norwegian Competition Authority for 2020, the Authority was asked to prioritise the investigation into global platform players that may be in breach of the Norwegian Competition Act.[55] Former Finance Minister Siv Jensen has also stated that it may be appropriate to introduce a special Norwegian digital tax if the work on an international framework for the taxation of IT giants under the auspices of the OECD does not produce any results in 2020.[56]

[55] The Norwegian Ministry of Trade, Industry and Fisheries (2020)
[56] Vollan, Mari Brenna (2020)

TRACKING ON PUBLIC SECTOR WEBSITES

The Norwegian Board of Technology has examined a number of public sector websites, using the tool Blacklight[57] in order to look into how users are tracked. When a URL is entered in the tool, Blacklight will examine the website in question and look for processes that can be identified as tracking online usage, as well as which companies receive information about such use.

The Norwegian Board of Technology has looked into whether the websites:

- use Google Analytics
- have the *remarketing audiences* feature enabled
- share data with the DoubleClick advertising exchange
- use Facebook Pixel
- share data with companies that perform keylogging or recording of website visits.

In addition to the technical examination using Blacklight, we have also read the privacy policies of the websites to look at how the businesses describe the tracking themselves and whether they have taken any steps to minimise the collection and sharing of data.

The Norwegian Board of Technology has examined 41 public sector websites, including those of the government, public agencies and a selection of

[57] https://themarkup.org/blacklight

municipalities. The examination was conducted during the autumn of 2020, with an update in January 2021.

Of all the websites examined, only the Norwegian Data Protection Authority, the Norwegian State Educational Loan Fund and the Norwegian Competition Authority were found not to share data with any other parties. The majority shared data with Alphabet (Google's parent company), either via Google Analytics, Google Tag Manager or the DoubleClick advertising exchange. Facebook Pixel is less common and was used only by four of the websites.

None of the websites used specific tools for keylogging. However, 14 of the websites did use Hotjar, which is a popular tool for recording website visits. In many cases, this can also involve the recording of text that is entered on the website.[58]

WEBSITE	TRACKING TECHNOLOGY				
	Google			**Facebook Pixel**	**Recording of website visits**
	Google Analytics	*Remarketing Audiences*	*DoubleClick*		
The Norwegian Labour Inspection Authority	X				
The Norwegian Directorate for Children, Youth and Family Affairs	X	X	X		X
The Municipality of Bergen	X				

[58] Wakefield, Jane (2017)

The Norwegian Data Protection Authority					
The Norwegian Digitalisation Agency	X				
The Norwegian Directorate of eHealth	X	X	X		
The Norwegian Directorate for Civil Protection	X				
The Norwegian Institute of Public Health	X				
The Norwegian Consumer Council	X				
The Norwegian Consumer Authority	X	X	X		X
The Research Council of Norway	X	X	X	X	X
The Norwegian Directorate of Health	X				X
Helsenorge.no*					
The Norwegian Board of Health Supervision	X				
The Norwegian State Housing Bank	X				
Innovation Norway	X	X	X	X	X

The Norwegian Directorate of Integration and Diversity	X				
Skills Norway				X	
The Norwegian Competition Authority					
The Equality and Anti-Discrimination Ombud	X	X	X		
The Norwegian State Educational Loan Fund					
The Norwegian Media Authority	X	X	X	X	
The Norwegian National Security Authority	X	X	X		
The Norwegian Labour and Welfare Administration	X				X
Norge.no	X				
The Norwegian System of Patient Injury Compensation	X				X
Oslo University Hospital	X				
The Municipality of Oslo	X		X		X

Politiet.no	X				
Regjeringen.no	X				
The Norwegian Parliamentary Ombudsman	X	X	X		
The Norwegian Tax Administration	X				
The Norwegian Public Roads Administration	X	X	X		X
The Municipality of Stavanger	X	X	X		X
The Norwegian Parliament (Stortinget)	X	X	X		X
The Municipality of Tromsø	X				
The Municipality of Trondheim	X	X	X		
Utdanning.no	X	X	X		X
The Norwegian Directorate of Immigration	X	X	X		X
The Norwegian Immigration Appeals Board	X				
The Norwegian Directorate of Elections	X	X	X		

*Helsenorge.no does not use the most common tracking technologies from Google and Facebook. Similar tools from Adobe are used instead.

MOST SERVICES TRACK USERS

Google is the dominant international player within web traffic analytics. This is also the case in the Norwegian public sector. Of the 41 websites we examined, 36 used one or more services from Google.

All of these 36 used Google Analytics and 17 of the websites also sent data to DoubleClick (Google's advertising exchange). None of these 17 websites provide information in their privacy policies about why this is done or what sort of data is shared.

Both the volume of data held by Google and the retention periods are problematic. For example, a visit to the Norwegian State Housing Bank website would result in data being sent to DoubleClick and the Google-owned YouTube for use in targeted marketing. If you do not delete cookies from your web browser, Google reserves the right to leave them active for a full 17 years.

Markedsføring (6)

Markedsførings-informasjonskapsler brukes til å spore besøkende på tvers av hjemmesider. Hensikten er å vise annonser som er relevante og engasjerende for den enkelte brukeren, og dermed mer verdifulle for utgivere og tredjeparts-annonsører.

Navn	Leverandør	Formål	Utløpsdato
YSC	.youtube.com	Samler informasjon om brukerne og deres aktivitet på nettstedet gjennom innebygde videospillere med det formål å levere målrettet annonsering.	Session
IDE	.doubleclick.net	Brukes til nettbasert markedsføring ved å samle inn informasjon om brukerne og deres aktivitet på nettstedet. Informasjonen brukes til å målrette annonsering til brukeren på forskjellige kanaler og enheter.	ett år
GPS	.youtube.com	Samler informasjon om brukerne og deres aktivitet på nettstedet gjennom innebygde videospillere med det formål å levere målrettet annonsering.	30 minutter
VISITOR_INFO1_LIVE	.youtube.com	Samler informasjon om brukerne og deres aktivitet på nettstedet gjennom innebygde videospillere med det formål å levere målrettet annonsering.	6 måneder
NID	.google.com	Lagrer dine seneste søk, dine foregående interaksjoner med annonsørenes annonser eller søkeresultater, samt dine besøk på en annonsørs nettsted for å kunne målrette annonser til deg på Google.	6 måneder
CONSENT	.google.com	Lagrer dine seneste søk, dine foregående interaksjoner med annonsørenes annonser eller søkeresultater, samt dine besøk på en annonsørs nettsted for å kunne målrette annonser til deg på Google.	17 år

Screenshot from the Norwegian State Housing Bank's privacy policy. Retrieved 20 November 2020.

The fact that Google has a presence on such a large proportion of public sector websites is problematic. When several of these websites are also clearly linked to commercial advertising services, these challenges become even greater. It is difficult to imagine that the various agencies have a rationale for this that outweighs the privacy of users.

The *remarketing audiences* feature has been developed to present targeted ads to customers who have previously visited a website. An example of this is when you are presented with advertisements on various websites for a product you have previously looked at in an online store. Of the websites we examined, we found that 16 used this feature, including the Municipality of Trondheim, the Norwegian Directorate of Immigration, the Norwegian Public Roads Administration and Stortinget.no.

The Norwegian Directorate for Children, Youth and Family Affairs is the only agency to address this matter in its privacy policy and attempts to provide an explanation for the use:

> *"One of the social missions of Bufdir is to recruit foster families to house children and young people in need. We therefore need to establish contact with as many potential foster parents as possible. For this reason, we use cookies on the section of bufdir.no that relates to foster homes. This makes it possible for us to present relevant content with more information about fostering on other websites to those who have shown interest within a specific period of time. This type of cookie is also used on the everyday parenting and family counselling offices pages."*[59]

Even though the agency is seeking to solve a real challenge in the recruitment of foster parents, it is nevertheless unfortunate that visits to certain parts of the Bufdir website are passed onto and further used by the digital advertising industry.

Through the tracking of users and the free tools from the tech giants, several public sector agencies are also directly counteracting their own social missions. The Norwegian Parliamentary Ombudsman, for example, uses Google Analytics and remarketing audiences and shares data with the DoubleClick advertising exchange. This is not consistent with their mission to safeguard the rights of the individual in matters relating to public authorities.[60]

INADEQUATE OR LACKING INFORMATION ABOUT TRACKING

It is a known issue that terms of use and agreements are so long and complicated that the majority of people do not read them. The Norwegian Consumer Council has previously shown how it would have taken 24 hours to read the terms of a selection of the most commonly used apps on a phone out loud.[61]

The amount of text and the high levels of complexity therefore make it virtually impossible to know what you are consenting to. In the public sector, there are rarely alternative service providers that can be used, and you have no option but to accept the terms in order to access the services. All of the websites

[59] Retrieved from the privacy policy at bufdir.no
https://bufdir.no/Personvern/personvern_og_cookies_pa_bufdir.no/
[60] https://www.sivilombudsmannen.no/om/
[61] The Norwegian Consumer Council (2016b)

examined by the Norwegian Board of Technology have their own privacy policies but in many cases, they also reference the provider's own guidelines:

> *"We use analytics tools from Google Analytics and Hotjar on our main website, www.forskningsradet.no. By closing the message banner that is displayed when you visit the website, you consent to our use of cookies and you consent to the use of Google Analytics's guidelines for privacy in relation to this processing."*

It is therefore highly challenging for users to gain an insight into the actual consequences of the data collection and processing, as they need to visit the website providers in order to familiarise themselves with this.

The Norwegian Consumer Authority, which, among other things, works precisely on preventing unreasonable terms in contracts,[62] also uses tracking tools from Google. In its privacy policy, the Norwegian Consumer Authority references the Google privacy policy and states that users of their website also have to consent to Google's terms.

On certain websites, the privacy policy contains no information about cookies at all, such as the websites of the Norwegian Directorate of Civil Protection and the Norwegian Directorate of Elections, even though the Blacklight tool shows that the websites contain several cookies.

Another common example is for the websites to list the cookies that are used but to fail to mention that they also use Facebook Pixel, such as on the part of Skills Norway and the Norwegian Media Authority. Given Facebook's somewhat murky reputation when it comes to the processing of personal data, it is unfortunate for the Norwegian Media Authority, which, among other things, is tasked with guiding children and young people in the use of digital media[63], to share tracking data with Facebook.

Other websites include a lot of information in their privacy policies but with such a complex presentation that it is almost incomprehensible. Innovation Norway, for example, presents a long table in English listing the cookies that are used and the associated purpose but without any further explanation as to what this entails.[64]

---

[62] https://www.forbrukertilsynet.no/om-forbrukertilsynet
[63] https://www.medietilsynet.no/om/vare-oppgaver/
[64] See the overview here https://www.innovasjonnorge.no/no/privacydeclaration/cookies/

Even in cases where the privacy policy explains matters in simple terms, it can still be difficult for the user to know what online tracking actually involves. A single visit to a website might not seem important and may be considered an insignificant piece of information to give away. But when a complete overview of all online activities can be accessed by a dominant player, this picture becomes extremely detailed.

PUBLIC SECTOR CONTRIBUTING TO UNDESIRABLE MARKET DOMINANCE

The surveillance economy is dominated by a handful of international companies, of which Google and Facebook are two of the largest. Work is being undertaken on competition policy both in Norway and internationally in order to limit the dominance on the part of the major internet companies.

As described above, this dominance creates a monopoly-like market situation that can prevent other companies from becoming established, thereby hindering innovation. The same trend can also be seen when it comes to website statistics services. Google Analytics is so dominant that it is difficult for other, perhaps more privacy-friendly actors, to establish themselves in this field. In addition, it is difficult to compete against a company that offers its services for free.

Innovation Norway aims to contribute towards innovation in business and growth for Norwegian companies. Nevertheless, they use free tools from both Google and Facebook on their websites, which counteracts innovation in the digital economy. Even the Norwegian Digitalisation Agency, which, among other things, is tasked with contributing to the appropriate digitisation of society and advising the public sector on matters relating to innovation, makes use of services from Google.

In light of the political desire to counteract the digital dominance of the major companies, public sector agencies should not support the international companies and business models of the surveillance economy.

WHAT CAN BE DONE?

The public sector should lead the way and take active steps to minimise the collection of data and tracking of users online.

The surveillance economy has already gone too far. The business model in which user data is bought and sold several times a day constitutes an invasion of privacy that is deeply problematic. There is a need for governance and enforcement to protect personal data and put an end to data being used as the currency in a global industry.

The public sector should take the lead and assume particular responsibility for providing citizens with strong digital services – without allowing commercial players to be able to look over our shoulders.

MINIMISE DATA COLLECTION AND PROVIDE PROPER INFORMATION

Several of the websites argue that they rely on the collection of data in order to offer user-friendly websites. User-friendliness is a key aspect of the digitisation of public services and the analysis of user data is, understandably, an important element in being able to offer this.

Nevertheless, it remains problematic that many websites appear to consider this more important that the protection of users' privacy. When most of the websites also use free services from the major players in the surveillance economy, this argument is weakened even further.

At the same time, it is extremely difficult, time-consuming and expensive to create a website, newsletter or other digital service without tracking users at all. The Markup, which developed the tool that the Norwegian Board of Technology used in its work on this report, has spent more than NOK 500,000 to develop its own zero-tracking tools because it cannot find such solutions on the market.[65] Existing tools for building websites and newsletters, playing videos and collecting donations generally track users without any option to fully disable such tracking.

Here, the public sector, as a player with great purchasing power, can lead the way and actively choose and encourage the development of solutions and tools that adhere to the principles of privacy. In this way, minimal data could be collected and only for very specific purposes. Privacy-friendly solutions should become a competitive advantage rather something that is lacking in the market.

If data is collected at all, it is important to be able to explain the purpose of the tracking in a clear and simple manner. This is far from the case today. The public sector should therefore strive to comply with the requirement set down in the Norwegian Electronic Communications Act to provide clear information about the collection and use of data through cookies. Most of the websites we have examined have privacy policies that include only very general descriptions of how they use cookies and tracking tools.

THE STATE SHOULD PAY WITH MONEY AND NOT CITIZENS' DATA.

Google does not offer its analytics tools for free out of the kindness of its heart, but because they see the value of the data collected using the tool.

Even though Google Analytics is the most prevalent solution for the analysis of website visits, alternatives do exist.[66] The fact that these alternatives cost money should not be a reason for us to continue supplying data about ourselves to Google and Facebook.

The public sector should make an active choice not to participate in the surveillance economy and should pay for the tools they use with money – not citizens' data. This could also lead to stimulation of the market through increased demand for privacy-friendly solutions.

[65] Angwin, Julia (2020)
[66] Schwab, Katharine (2019)

CONSIDER A BAN ON MICROTARGETING

One of the reasons for data collection is for use in targeted marketing. There are already many examples of how such personalisation and microtargeting techniques have influenced democracies and social structures around the world.[67] Electoral intervention, disinformation campaigns and covert discrimination are only some examples.

The European Parliament refers to such detailed targeted marketing as one of the most destructive practices online today. It has asked the European Commission to present proposals for how this can be more effectively governed and has, among other things, proposed how to perform a phase-out and eventually a ban on microtargeting.[68] In Norway, the Liberal Party has advocated in favour of such a ban in its proposed party platform.[69]

There are already alternative methods available for digital advertising that could replace the use of personal data for targeted marketing. So-called contextual advertising means that adverts are placed based on the content of a website, not on who the user is.[70] For example, an advertisement for Norwegian carrots could be placed with a recipe for a carrot cake or an advertisement for audiobook streaming could be placed in an interview with an author.[71]

A ban on the use of personal data in ads could also help improve the competitive situation. By depriving companies such as Google and Facebook of their greatest advantage (personal data), other companies in the advertising market would be able to compete on more equal terms.

[67] Bayer, Judit (2019)
[68] European Parliament (2020)
[69] Veberg, Anders (2020)
[70] Iwańska, Karolina (2020)
[71] These examples have been taken from Kobler, a Norwegian contextual advertising company.

LITERATURE

Angwin, Julia (2020) *Paying the Privacy Price*. Newsletter from The Markup, December 12th 2020.
Retrieved from: https://www.getrevue.co/profile/themarkup/issues/paying-the-privacy-tax-298830

Baisotti, Valentina (2019) *Måten du taster på kan avsløre mye om hvem du er*. NRK.no, January 23rd 2019.
Retrieved from: https://www.nrk.no/vestland/maten-du-taster-pa-kan-avslore-mye-om-hvem-du-er-1.14392572

The Norwegian Directorate for Children, Youth and Family Affairs (undated) *Personvern og cookies på Bufdir.no*. Retrieved October 2020.
Retrieved from: https://bufdir.no/Personvern/personvern_og_cookies_pa_bufdir.no/

Bayer, Judit (2019) *Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States*. EUs Policy Department for Citizens' Rights and Constitutional Affairs, February 2019.
Retrieved from: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU(2019)608864_EN.pdf

Brin, Sergey og Lawrence Page (1998) *The Anatomy of a Large-Scale Hypertextual Web Search Engine*
Retrieved from: http://infolab.stanford.edu/~backrub/google.html

Briz, Nock (2018) *This is Your Digital Fingerprint*. Mozilla.org, July 26th 2018
Retrieved from: https://blog.mozilla.org/internetcitizen/2018/07/26/this-is-your-digital-fingerprint/

Chen, Brian X. (2019) *«Fingerprinting» to Track Us Online Is on the Rise. Here's What to Do*. New York Times, July 3rd 2019.
Retrieved from: https://www.nytimes.com/2019/07/03/technology/personaltech/fingerprinting-track-devices-what-to-do.html

Christl, Wolfie (2017) *How Companies Use Personal Data Against People*. Cracked Lab, October 2017.
Retrieved from: https://crackedlabs.org/en/data-against-people

Consumer Reports (2020) *Platform Perceptions. Consumer Attitudes On Competition and Fairness in Online Platforms.*
Retrieved from: https://advocacy.consumerreports.org/wp-content/uploads/2020/09/FINAL-CR-survey-report.platform-perceptions-consumer-attitudes-.september-2020.pdf

Court of Justice of the European Union (2020) *Judgment in Case C-311/18. Data Protection Commissioner v Facebook Ireland and Maximillian Schrems*
Retrieved from: https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf

Drange, Jan Morgen og Vebjørn Søndersrød (2020) *Digital markedsføring i Norge i skvis mellom EU og USA*. Dagens Næringsliv, September 23rd 2020.
Retrieved from: https://www.dn.no/innlegg/markedsforing/annonsering/anfo-annonsorforeningen/innlegg-digital-markedsforing-i-norge-i-skvis-mellom-eu-og-usa/2-1-879751

Ekeberg, Ingrid (2019) *Amedia og Aller Media tar opp annonsekampen mot Google og Facebook: Oppretter eget selskap.* Dagens Næringsliv, June 21st 2019.
Retrieved from: https://www.dn.no/reklame/aller-media/amedia/dag-sorsdahl/amedia-og-aller-media-tar-opp-annonsekampen-mot-google-og-facebook-oppretter-eget-selskap/2-1-625425

eMarketer (2020) *Digital Ad Spending Worldwide, by company, 2019-2020.*
Retrieved from: https://www.emarketer.com/chart/234937/digital-ad-spending-worldwide-by-company-2019-2022-billions

European Parliament (2020) *REPORT with recommendations to the Commission on a Digital Services Act: adapting commercial and civil law rules for commercial entities operating online (2020/2019(INL))*.
Retrieved from: https://www.europarl.europa.eu/doceo/document/A-9-2020-0177_EN.pdf

Facebook (undated) *Find out What's Popular on Your Website with the Facebook Pixel*. Read October 2020.
Retrieved from: https://www.facebook.com/business/learn/lessons/overview-of-how-facebook-pixels-work?course_id=314938442554416&curriculum_id=726377631115881

Federal Trade Commission (2020) *FTC sues Facebook for Illegal Monpolization*. Federal Trade Commision, December 9th 2020.
Retrieved from: https://www.ftc.gov/news-events/press-releases/2020/12/ftc-sues-facebook-illegal-monopolization

Fedorovicius, Julius (2020) *Google Tag Manager vs Google Analytics: What's the difference?* AnalyticsMania, July 16th 2020.
Retrieved from: https://www.analyticsmania.com/post/google-tag-manager-vs-google-analytics/

Foroohar, Rana (2019) *Don't be evil. How Big Tech betrayed its founding principles – and all of us*. New York, Penguin Random House

Google (udatert) *Data sharing settings*. Hentet oktober 2020
Retrieved from: https://support.google.com/analytics/answer/1011397/

Jørgenrud, Marius (2013) *Datatilsynet godtar Google Analytics*. Digi.no, February 6th 2020.
Retrieved from: https://www.digi.no/artikler/datatilsynet-godtar-google-analytics/198644

Iwańska, Karolina (2020) *TO TRACK OR NOT TO TRACK? Towards privacy-friendly and sustainable online advertising*. Panoptykon Foundation, November 2020
Retrieved from: https://en.panoptykon.org/privacy-friendly-advertising

Jørgenrud, Marius (2012) *Ulovlig å bruke Google Analytics*. Digi.no, August 20th 2012.

Retrieved from: https://www.digi.no/artikler/ulovlig-a-bruke-google-analytics/204856

Kassner, Michael (2017) *Session-replay scripts disrupt online privacy in a big way*. Tech Republic, September 26th 2017.
Retrieved from: https://www.techrepublic.com/article/session-replay-scripts-are-disrupting-online-privacy-in-a-big-way/

Kaspersky (udatert) *What is Keystroke Logging and Keyloggers?* Read October 2020.
Retrieved from: https://www.kaspersky.com/resource-center/definitions/keylogger

Kemp, Katharine (2019) *Concealed Data Practices and Competition Law: Why Privacy Matters*. UNSW Law Research Paper No. 19-53 (2019) Retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3432769#

Lomas, Natasha (2020) *IAB Europe's ad tracking consent framework found to fail GDPR standard*. TechCrunch, October 16th 2020.
Retrieved from: https://techcrunch.com/2020/10/16/iab-europes-ad-tracking-consent-framework-found-to-fail-gdpr-standard/

McDougall, Simon (2020) *Blog: Adtech - the reform of real time bidding has started and will continue*. Information Commissioner's Office, January 17th 2020.
Retrieved from: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/01/blog-adtech-the-reform-of-real-time-bidding-has-started/

Ministry of Trade, Industry and Fisheries (2020) *Konkurransetilsynet (KT) – tildelingsbrev 2020*.
Retrieved from: https://konkurransetilsynet.no/wp-content/uploads/2020/01/Tildelingsbrev-2020-Konkurransetilsynet.pdf

NOYB (2020) *101 Complaints on EU-US tranfers filed*.
Retrieved from: https://noyb.eu/en/101-complaints-eu-us-transfers-filed

Paul, Kari (2020) *Texas and other states sue Google for abusing "monopolistic power"*. The Guardian, December 16th 2020

Retrieved from: https://www.theguardian.com/technology/2020/dec/16/google-lawsuit-texas-monopolistic-power

Schwab, Katharine (2019) *It's time to ditch Google Analytics*. Fast Company, February 1st 2019.
Retrieved from: https://www.fastcompany.com/90300072/its-time-to-ditch-google-analytics

Shead, Sam (2019) *Facebook owns the four most downloaded apps of the decade*. BBC, December 18th 2019.
Retrieved from: https://www.bbc.com/news/technology-50838013

Solsman, Joan E. (2018*) YouTube's AI is the puppet master over most of what you watch*. Cnet, January 10th 2018.
Retrieved from: https://www.cnet.com/news/youtube-ces-2018-neal-mohan/

Statista (2020) *The 100 largest companies in the world by market capitalization in 2020*.
Retrieved from: https://www.statista.com/statistics/263264/top-companies-in-the-world-by-market-capitalization/

Steel, Emely (2013) *Financial worth of data comes in at under a penny a piece*. Financial Times, June 12th 2013.
Retrieved from: https://www.ft.com/content/3cb056c6-d343-11e2-b3ff-00144feab7de

Subcommittee on antitrust, commercial and administrative law of the committee on the judiciary (2020) *Investigation of competition in digital markets*.
Retrieved from: https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf

The Competition and Markets Authority (2020) *Online platforms and digital advertising. Market study final report*.
Retrieved from: https://assets.publishing.service.gov.uk/media/5efc57ed3a6f4023d242ed56/Final_report_1_July_2020_.pdf

The European Consumer Organisation (2019) *Access to consumers' data in the digital economy*.
Retrieved from: https://www.beuc.eu/publications/beuc-x-2019-068_european_data_policy.pdf

The Norwegian Board of Technology (2016) *Personvern. Tilstand og trender*.
Retrieved from: https://teknologiradet.no/publication/personvern-trender-2016/

The Norwegian Communications Authority (2020) *Informasjon-skapsler/cookies*.
Retrieved from: https://www.nkom.no/internett/informasjonskapsler-cookies

The Norwegian Competition Authority (2019) *Cookie Policy*.
Retrieved from: https://konkurransetilsynet.no/cookie-policy/

The Norwegian Competition Authority (2017) *Strategiplan for Konkurransetilsynet 2017-2021*.
Retrieved from: https://konkurransetilsynet.no/wp-content/uploads/2019/07/Strategiplan-2017-2021.pdf

The Norwegian Consumer Council (2020) *Out of control. How consumers are exploited by the online advertising industry*.
Retrieved from: https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf

The Norwegian Consumer Council (2018) *Facebook og Google manipulerer oss til å dele personinformasjon*.
Retrieved from: https://www.forbrukerradet.no/siste-nytt/facebook-og-google-manipulerer-oss-til-a-dele-personinformasjon/

The Norwegian Consumer Council (2016a) *Norske kommuner svikter innbyggernes personvern*.
Retrieved from: https://www.forbrukerradet.no/vi-mener/2015/fpa-digital-2015/norske-kommuner-svikter-innbyggernes-personvern/

The Norwegian Consumer Council (2016b) *Du må lese over en kvart million ord med appvilkår*.
Retrieved from: https://www.forbrukerradet.no/vi-mener/2015/fpa-digital-2015/du-ma-lese-over-en-kvart-million-ord-med-appvilkar/

The Norwegian Data Protection Authority (2021) *Varsel om overtredelsesgebyr til Grindr*.

Retrieved from: https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2021/varsel-om-overtredelsesgebyr/

The Norwegian Data Protection Authority (2020) *Privacy Shield-avtalen mellom USA og EU/EØS er opphevet*.
Retrieved from: https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2020/privacy-shield-avtalen-mellom-usa-og-eueos-er-opphevet/

The Norwegian Data Protection Authority (2018) *Verktøy for statistikk og analyse av nettsider*.
Retrieved from: https://www.datatilsynet.no/personvern-pa-ulike-omrader/internett-og-apper/webanalyse/

The Norwegian Digitalisation Agency (undated) *Digitalt førstevalg*. Read October 2020.
Retrieved from: https://www.difi.no/fagomrader-og-tjenester/digitalt-forstevalg

The Verge (2019) *What is a tracking pixel and can strangers really spy on me through email? Everything you need to know about the invisible e-mail tool that tracks you*. The Verge, July 3rd 2019
Retrieved from: https://www.theverge.com/2019/7/3/20681508/tracking-pixel-email-spying-superhuman-web-beacon-open-tracking-read-receipts-location

Veberg, Anders (2020) *Venstre vil forby målrettet reklame mot barn og unge*. Aftenposten, November 23rd 2020.
Retrieved from: https://www.aftenposten.no/kultur/i/nA9Xzo/venstre-vil-forby-maalrettet-reklame-mot-barn-og-unge

Véliz, Carissa (2020) *Privacy is Power. Why and how you should take back control of your data*. London, Penguin

Vollan, Mari Brenna (2020) *Åpner for norsk it-skatt*. Klassekampen, January 13th 2020.
Retrieved from: https://arkiv.klassekampen.no/article/20200113/ARTICLE/200119987

W3Techs (2020) *Usage statistics and market share of Google Analytics for websites*.
Retrieved from: https://w3techs.com/technologies/details/ta-googleanalytics

Wakefield, Jane (2017) *More than 480 web firms record "every keystroke"*. BBC, November 21st 2017.
Retrieved from: https://www.bbc.com/news/technology-42065650

Whatagraph (2019) *What is a tracking pixel and how does it work?*
Retrieved from: https://whatagraph.com/blog/articles/tracking-pixel

Which? (2018) *Control, Alt or Delete? The future of consumer data.*
Retrieved from: https://www.which.co.uk/policy/digital/2659/control-alt-or-delete-the-future-of-consumer-data-main-report

White Paper no. 27 to the Storting (2015–2016) *Digital agenda for Norge — IKT for en enklere hverdag og økt produktivitet*. Melding til Stortinget April 15th 2016.
Retrieved from: https://www.regjeringen.no/no/dokumenter/meld.-st.-27-20152016/id2483795/

Wired (undated) *The Cambridge Analytica Story, Explained*. Read Ocktober 2020.
Retrieved from: https://www.wired.com/amp-stories/cambridge-analytica-explainer/

Zuckerman, Ethan (2014) *The Internet's Original Sin. It's not too late to ditch the ad-based business model and build a better web*. The Atlantic August 14th 2014.
Retrieved from: https://www.theatlantic.com/technology/archive/2014/08/advertising-is-the-internets-original-sin/376041/