THE GREAT DATA RACE

How commercial utilisation of personal data challenges privacy. Report, november 2015

Datatilsynet

Content

Summary 5
Introduction 7
Automated ad trading: processes and players 10
Collection of data 19
Building profiles 25
What is the legal picture? 29
Privacy challenges 39
Recommendations 45
Bibliography 51
Appendix 1: Overview of third-party Norwegian online newspapers 54
Appendix 2: Description of third-party players present on Norwegian websites 60
Appendix 3: Glossary 65

Summary

A data race is taking place in the media and advertising industry. New technology and the ability to gather and analyse large volumes of data are changing the ways in which advertisers reach consumers. Consumers were once split into demographic groups, which were targeted via mass media. Today we are bought and sold one by one on global ad exchanges. This results in marketing which is highly targeted and which presupposes that the marketers have a thorough understanding of our habits, interests, tastes and network of contacts, in order to have the greatest impact.

Google and Facebook dominate the market in automated ad trading because they have such an enormous amount of information about us. In Norway and Europe big media companies are currently building their own platforms for programmatic technology in an attempt to take on the global giants. The company who has the most data and the best technology is the winner of the data race.

Every time we visit a website we don't engage with just one company, but many companies at the same time. As well as the publisher who owns the site, ad exchanges, demand side and supply side platforms, ad networks, data brokers and data management platforms are present using various tracking tools. Our report reveals that on average 43 different companies have a presence on Norwegian online newspapers and record what we do. Between 100 and 200 cookies were stored on our web browser when visiting the front page of six Norwegian newspapers.

As a user, you may first notice the result of the cookies placed on your browser when the same ad starts following you around the Internet. The information that is gathered is used to build up comprehensive profiles about us. The more detailed the profiles are, the greater their market value.

If we lose control of our own personal information, we also lose the ability to define who we are ourselves. No sector in the world knows more about us than the advertising industry. At the same time, we have very little insight into how these companies use the information they have about us.

Privacy must not only give the individual protection against constant surveillance by the authorities, but also protect us against private companies monitoring everything we do. The individual is very small compared to a large corporation. Privacy legislation must redress some of this imbalance of power. Because the advertising industry is so lacking in transparency, however, individuals have limited opportunities to exercise their fundamental right to privacy in their dealings with it.

The information asymmetry that characterises the market is a form of market failure. When consumers have no knowledge about what is going on, they cannot demand services that offer better privacy. The uneven distribution of information results in a competitive situation, which encourages the market players to use methods increasingly invasive of privacy. When we surf the Internet we want quick and easy access to the services we are searching for. We will almost automatically accept everything we are asked to accept. Making the processing of personal data subject to consent does not, then, have the intended effect. When we let individuals decide for themselves, the individual must stand alone against big and powerful players who are in reality able to dictate what the individual must consent to.

The Norwegian Data Protection Authority will work to increase transparency and openness in the advertising market, ensure genuine freedom of choice for users and give the user more control over his or her own personal information. The most important recommendations and measures we propose in the report are as follows:

- Publishers (such as newspapers) must take responsibility for the third-party players they allow access to their pages.
- Companies engaged in the collection of personal data for profiling and marketing purposes must base the processing of the data on an active consent from the users
- Publishers must give all users access to their services, including those who do not consent to their information being collected.
- The privacy policies must be improved. They must be short and easy to follow, but must also include clear information about what data is collected, how it is processed and whether other players have access to the information.
- Publishers, media agencies and advertisers must join forces to produce guidelines that may contribute to greater openness and transparency about the nature of targeted advertising.

Introduction

A data race is currently taking place in the media and advertising industry. New technology and the ability to gather and analyse large volumes of data are changing the ways in which advertisers reach consumers. Consumers were once divided into demographic groups, which were targeted via mass media. Today we are bought and sold one by one on global ad exchanges. This results in marketing which is highly targeted and which presupposes that the marketers have a thorough understanding of our habits, interests, tastes and network of contacts, in order to have the greatest impact. Computers and algorithms now has taken over the sale of advertising space. This new way of trading ad space is called programmatic buying.

Currently, you are exposed to targeted advertising when browsing the web, but before long you will also experience it when watching TV.

Google and Facebook dominate the market in automated ad trading because they have such an enormous amount of information about us. In Norway and Europe, big media companies are currently building their own platforms for programmatic trading in order not to lose out in competition with foreign players. The company who has the most data and the best technology is the winner of the data race.

The harvesting of personal data takes place on a grand scale, and it takes place out of sight. We have no idea what is happening behind the scenes when we visit a website. The market is characterised by information asymmetry. Hundreds of companies know a great deal about us, whilst we are unaware of who they are and what they know about us. This is the main reason why the Norwegian Data Protection Authority has chosen to take a closer look at the advertising industry's collection and use of personal data. Our right to self-determination is challenged when we do not have control over how our personal data are utilised.

In this report we want to turn the spotlight onto the consequences for privacy when more and more information about our activities and interests is gathered and traded like a commodity.

The objective is to contribute knowledge about a complex market. It is difficult to gain an overview of this market, and although it affects everyone, very few people have any insight into it. Acquiring more knowledge is the first step on the way to creating greater openness and transparency in the advertising market, and giving individuals greater control over their own personal data.

Increased knowledge is also important if we are to spark off a debate on these issues. The Norwegian Data Protection Authority wishes the report to contribute to a discussion about how far marketers can go in mapping individuals in order to sell goods and services. Do consumers want personalised content and advertising at any price?

In the course of working on this report we have been in contact with the Norwegian Media Businesses' Association, the Norwegian advertisers' association and representatives of media agencies, media companies, market-analysis companies and advertisers.

Privacy – our right to be left alone

Marketing is about influencing people. This is not wrong in itself, but how far can companies actually go in influencing others before it is no longer acceptable? What methods is it acceptable to use in order to get someone to act in a particular way, or to get them to hold a certain opinion?

Some answers come easily: Using force is of course unacceptable. Lying, too. Is it however acceptable to gather a lot of information about someone in order to find out how just that person best can be influenced? That is a more difficult question.

From our perspective, this raises a very fundamental issue: To what extent does such a process respect the individual's right to a private life?

Respect for the individual's right to privacy is a fundamental principle in our society. It is fundamental enough to be considered a human right. The principle is expressly incorporated in the European Convention on Human Rights and embodied in the Norwegian constitution.

The right to privacy is at its core about how every individual is free and independent. We have an inherent freedom to make decisions about our own lives; it is part of our integrity or human worth.

What if you were tracked offline as you are online?

Let us conduct a mental exercise: you enter a large shopping centre where there are countless departments selling different products. As you enter, you are greeted by a man who explains that he works for a large company that assists the shopping centre with marketing and development.

He explains to you that he will follow you around to record which shops you enter, whether you meet anyone along the way, and more generally, what you do. The reason for this, the man explains, is that the centre wants to get to know its customers better so that it can organise its operations to better meet the customers' requirements. Relax, he says, I will stay at a distance, you won't notice that I'm there.

The man goes on to tell you that he needs some more information about you before you move on. He would like to record a few things about you so that the centre can distinguish you from all other users. He explains that they are doing this to recognise you the next time you visit. You will get advertising and offers adapted to your needs. Relax, he says again, we will not record your name or anything like that. We just take note of a number of your characteristics so that you become uniquely recognisable to us. Before you move on, the man says, in need you to consent to us recording and using all this information, as I explained.

You hesitate a little, and you then tell the man that you do not want all this information to be recorded, and that you would rather be left alone. The man answers that of course he respects your wishes, and that you do not have to if you do not want to. You are free to choose, but if you want to enter the centre you will have to accept that the information will be recorded and used. If you do not accept this, then unfortunately you will have to walk out of the door.

It is very likely that you would not accept this. It would be obvious to you what was about to happen, and you would most likely find it extremely invasive. You would also instinctively feel that it was unfair and unreasonable that you were not welcome unless you gave your consent to being followed. You would feel like your privacy had been violated.

Key to protecting privacy is allowing the individual to be in charge of his or her own affairs, without outside interference. In fact, the term «privacy» encompasses the individual's identity in the broadest sense. The individual must be free to shape her own identity and personality both in herself and in relation to other people. This freedom is about the absence of the watchful gaze. This goes regardless of whether it is the state or private companies that observe you.

People's lives play out in various arenas. We live our lives at work, at home, with our friends and family, on the way to our holiday homes, at the gym and so on. We have the right to a private life in all those different arenas.

A great deal of our lives also takes place on the Internet. This is a world in which we feel free. We do not feel like we are being watched over, nor do we experience any tangible physical discomfort. We do not feel invaded or restricted.

Nevertheless, we are always watched by someone on the Internet. A great deal of information about what we do in this world is recorded in detail, stored and used – and to a much greater extent than in any other arena. So even though we feel free, there is reason to ask whether we actually are. Is it freedom if almost everything we do is recorded? Is freedom the same as not experiencing discomfort or feeling invaded?

National authorities in any given state are responsible for ensuring the right to privacy according to both the European Convention on Human Rights and the Norwegian constitution. This responsibility is twofold. The authorities are for their own part obliged to respect the individual's privacy in its interaction with individual citizens. However, the state also has an obligation to ensure that individuals respect each others' privacy. They have a responsibility to prevent that one citizen invades the private life of another citizen, company or other legally defined parties. This responsibility is often referred to a proactive duty of care. The state must ensure that private life is respected when shaping and developing society.

In this report, we will start by giving a description of the market for automated ad trading, presenting the most important players in the value chain. In chapter three, we will go through various techniques for tracking and collecting information about individuals on the Internet. We will then look at the presence of third-party actors on some popular web sites in Norway. In chapter four, we look at how the collected information is used to build individual user profiles. What information does a profile contain, and how much value does a user have in pounds and pence? In chapter five, we go through the legal framework by which the advertising industry is bound. In chapter six, we discuss how the utilisation of personal data in the advertising industry challenges privacy. In chapter seven we summarise the most important points in the report and make some recommendations which may contribute to increasing openness and transparency in this market.

Automated ad trading: processes and players

The «black box» metaphor has been used to describe the market for automated ad trading, also called programmatic trading.[1] The expression is used because it is almost impossible for an outsider to gain an insight into how this market functions. Most people have no idea that every time they visit a website they are also sold to the highest bidder on an exchange. In this chapter, we will attempt to look inside the black box. We will describe how the process of buying and selling users of the ad exchanges functions and which players have a key role in this.

Transformations in the advertising market

Targeted advertising is not a new phenomenon. What is new is that the targeting is no longer directed at groups, but at the individual, and that the processes are automated and taken over by computers and algorithms. According to marketers, more has happened in the advertising industry in the last two years than in the previous 50.[2]

The development of ad exchanges makes it possible to buy and sell individual users in real time. The publishers put unique users up for sale on ad exchanges, and the advertiser with the highest bid gets to show ads to the person concerned. The most important change the ad exchanges have brought about is that the advertisers no longer buy *groups of users* bundled together by the publisher (for example, people who are interested in cars and motor sport). They can now buy users *one by one*, and decide themselves how much they want to pay for each individual user. This results in marketing which is very precisely pinpointed to individual interests.

Programmatic buying currently takes place on the Internet, but within a few years programmatic buying will also be the norm on other channels. This means that in a few years' time TV advertising will also be personalised, based on information gleaned from our viewing habits.[3]

In Europe the market for automated ad trading has grown rapidly since 2012. The United Kingdom leads the way, followed by France, the Netherlands and Sweden. Up until now, Norway has been lagging behind. Only 11 per cent of digital advertising sales in Norway took place on ad exchanges in 2014,[4] as opposed to 46 per cent in the United Kingdom.[5] Still, the Norwegian market is growing rapidly. Some forecasts show that 25 per cent of the digital advertising market in Norway will be programmatic in 2016.[6] Three out of four Norwegian newspapers put some of their ad spots and users up for sale on exchanges.[7]

How do the ad exchanges work?

The moment you type in the address of a web page and hit the return key, the start signal is given for a process that brings you in contact with a wide range of companies that gather information about you.

The system for selling ad space in real time on ad exchanges is referred to as «real time bidding». Real time bidding works as follows (for a more detailed description of the process see fact box on p. 14): When you (female aged 40, enjoys outdoor life and the owner of a holiday home) access an online newspaper, contact is established between your web browser and an ad server. The ad server notifies the publisher's *supply side platform* to fill in the empty ad spots on the page you are downloading with adverts. The supply side platform sends a notification to an *ad exchange* which invites advertisers to make a bid for you. The exchange sends information about you to *media agencies and demand side platforms* which are registered on the exchange.

1 Pasquale, Frank, «The Black Box Society. The Secret Algorithms That Control Money and Information», Harvard University Press, Cambridge, MA, 2015

2 The Economist, «Little Brother, Special Report on Advertising and Technology», 13.09.2014, http://www.ogilvydo.com/wp-content/uploads/2014/09/20140913_SR_MAILOUT.pdf

3 In order to position itself in the market for automated ad trading, Europe's largest broadcasting company, RTL, bought the ad exchange SpotXchange in 2014, ref: McCafferty&co, «European Media Conglomerate RTL Group Purchases SpotXchange, Paving the Way for Broadcasters to Keep Traditional Ad Dollars without the Traditional Ad Model», 01.03.2015, http://mccaffertyco.com/european-media-conglomerate-rtl-group-purchases-spotxchange-paving-the-way-for-broadcasters-to-keep-traditional-ad-dollars-without-the-traditional-ad-model/

4 Delta Projects, «Nåværende Programmatic status i Norge» [«Current Programmatic status in Norway»], 2014

5 http://www.iabeurope.eu/files/8914/2789/7694/IAB_Europe_Introduction_to_Programmatic_Webinar_slides.pdf

6 Delta Projects, «Nåværende Programmatic status i Norge» [«Current Programmatic status in Norway»], 2014

7 Delta Projects, «Nåværende Programmatic status i Norge», 2015,

This information may include information about your IP address, geographical location, income, gender, interests and the website you are visiting. Based on this information, combined with information about you which the advertiser and their demand side platform already has, they send a bid to the exchange. They know for example that you are looking for hiking shoes and a good offer on a wood burning stove. The bidder with the highest bid wins the right to show you an advert on the website when it loads. This all happens within milliseconds. The process may sound simple, but in reality it is highly complex and involves many hundreds of companies competing with each other. As well as buyers and sellers of ad space, a large group of companies which supply *data and data analysis* are also involved in the process.

The players

The advertising market on the Internet has always been very complex. Many actors are involved in the value chain between the advertisers and the publishers. The automation of media buying has however made this ecosystem even more complex. Over the past few years, a whole industry of companies has emerged which make a living out of assisting advertisers and publishers in the process of supplying the right advert to the right user.

To differentiate between the different agents in this market is challenging. Many companies play several roles in the value chain simultaneously. The market is still in the melting pot, and many of the roles and functions we see right now will perhaps be gone or have changed before long. Changes occur very quickly. However, even though technical solutions are replaced or changed, the key aspects of this new way of operating advertising sales will remain; users are no longer bought in bulk, but one by one on the basis of analyses of large volumes of data gathered about us.

In the table below, we have split the different agents in the value chain into four main categories: the open ad exchanges, buyers of advertising space, sellers of advertising space, and data and data-analysis providers. Some companies such as Google wear many hats and act as both seller and buyer of advertising space and as a provider of data and data analytics. Google stands out as easily the most powerful player in this market.

Ad exchanges

An ad exchange is a marketplace for the purchase and sale of advertising space, working in accordance with the same principles as stock exchanges. Ad exchanges are the link between advertisers and publishers, and are in the process of taking over the role previously played by ad networks. Ad exchanges were introduced in 2007

Annonsører	Buyers of ad space		Ad exchanges	Vendors of ad space		Konsument
	Media Agencies Group M-gruppen (WPP) Red Media Consulting (IPG) Carat og Vizeum (Dentsu/Aegis) PH, OMD og Starcom (Omnicom)	**Demand Side Platforms** DoubleClick Bid Manager (Google) Flurry (Yahoo) BrightRoll (Yahoo) Xaxis MediaMath Turn The Trade Desk Rocktfuel DataXu Appnexus	DoubleClick Adx (Google) Facebook Adx Microsoft Adx AppNexus (Microsoft) Right Media (Yahoo) OpenX AOL One Rubicon *Video:* AdapTV SpotXchange LiveRail (Facebook) *Mobil:* MoPub Smaato Flurry (Yahoo) BrightRoll (Yahoo)	**Supply Side Platforms** Schibsted Facebook Ex Admeld (Google) Rubicon Project Pubmatic Index Exchange Improve Digital Appnexus	**Publishers** Schibsted Dagbladet Polaris media Amedia Egemont Aller Startsiden Facebook Google	
	Trading desks Xaxis (WPP) Accuen (Omnicom) Vivaki (IPG) Amnet (Dentsu/Aegis)			**Ad networks** Google Adsense Scandinavian AdNetwork Webtraffic (Schibsted) Amedia Marked		
	Data and data analytics					
	Data Management Platforms Cxence Enreach Delta Projects Aggregate Knowledge, Adobe Audience Lotame, Acxiom, Adchemy, Datalogix, Demdex, Digilant, Epsilon, Experian, Digital, Lotame, Mediamath, Targetbase, Targusinfo, og [x + 1]	**Data brokers** BlueKai Acxiom Adobe Datalogix Experian Lotame	**Market research** TNS Gallup Norstat Nielsen Experian Comscore Kantar			

Table 1: Overview of the various players, grouped by role.

as a platform for real-time bidding. The exchanges function as a neutral platform where purchasers of advertising space can bid for users offered by the publishers.

An overwhelming number of users are available for sale on the ad exchanges. Every second 1.3 million users are sold on ad exchanges.[8] The number of transactions on the ad exchanges is 12 times greater than the number of transactions on the New York Stock Exchange.[9] All the biggest Internet companies - Facebook, Yahoo!, Google and Microsoft - own their own ad exchanges.

Vendors of advertising space

Publishers make their living from selling ad space to advertisers. Publishers include traditional newspaper publishers, news portals and landing pages, social media and search engines.

Traditional media companies have struggled financially in recent years. They are steadily losing their share of advertising revenue to Google and Facebook. In the US, Google's revenue from advertising is now greater than that of the press. . [10] Thanks to the extensive knowledge they have about their users, Google and Facebook can offer advertisers highly targeted advertising.

Media companies in Europe and Norway are currently investing heavily in technology in an attempt to take on the global giants. The three biggest Norwegian media companies - Schibsted, Polaris Media and Amedia - have introduced login solutions that can trace customers across the company's many news sites. By introducing login solutions the newspaper obtains very detailed knowledge about its customers. These data are valuable to advertisers who want to reach very specific target groups.

Publishers who want to put ad spots and users up for sale on the ad exchanges must use a **supply-side platform**. Supply-side platforms are forms of software that have been specially developed for this purpose. Admeld (Google), Rubicon Project, Pubmatic and Index Exchange are examples of companies that offer such software. These are the services Norwegian newspaper publishers use when they want to put users up for sale on the open ad exchanges.

Supply-side platforms can also function as ad exchanges and trade directly with invited media agencies and advertisers. In this capacity, they are referred to as private market places. There is a growing trend among publishers to establish private ad exchanges in order to gain greater control over their inventory. It is assumed that in future, private market places and open ad exchanges will be about the same size in terms of the number of transactions made.

The Norwegian media company Schibsted is fully occupied developing its own ad exchange platform. The company is working to get other Norwegian media - companies to sign up for this exchange rather than putting their users up for sale on the open ad exchanges.[11] The more newspapers they can attract to their platform, the more users they will be able to offer for sale and the more user data they will be able to gather and use for the purposes of targeted advertising. Similar alliances in which publishers collaborate on technology and data are being set up throughout Europe. [12]

8 Smith, Mike, «Targeted. How Technology Is Revolutionizing Advertising and the Way Companies Reach Consumers», Amacom, 2015

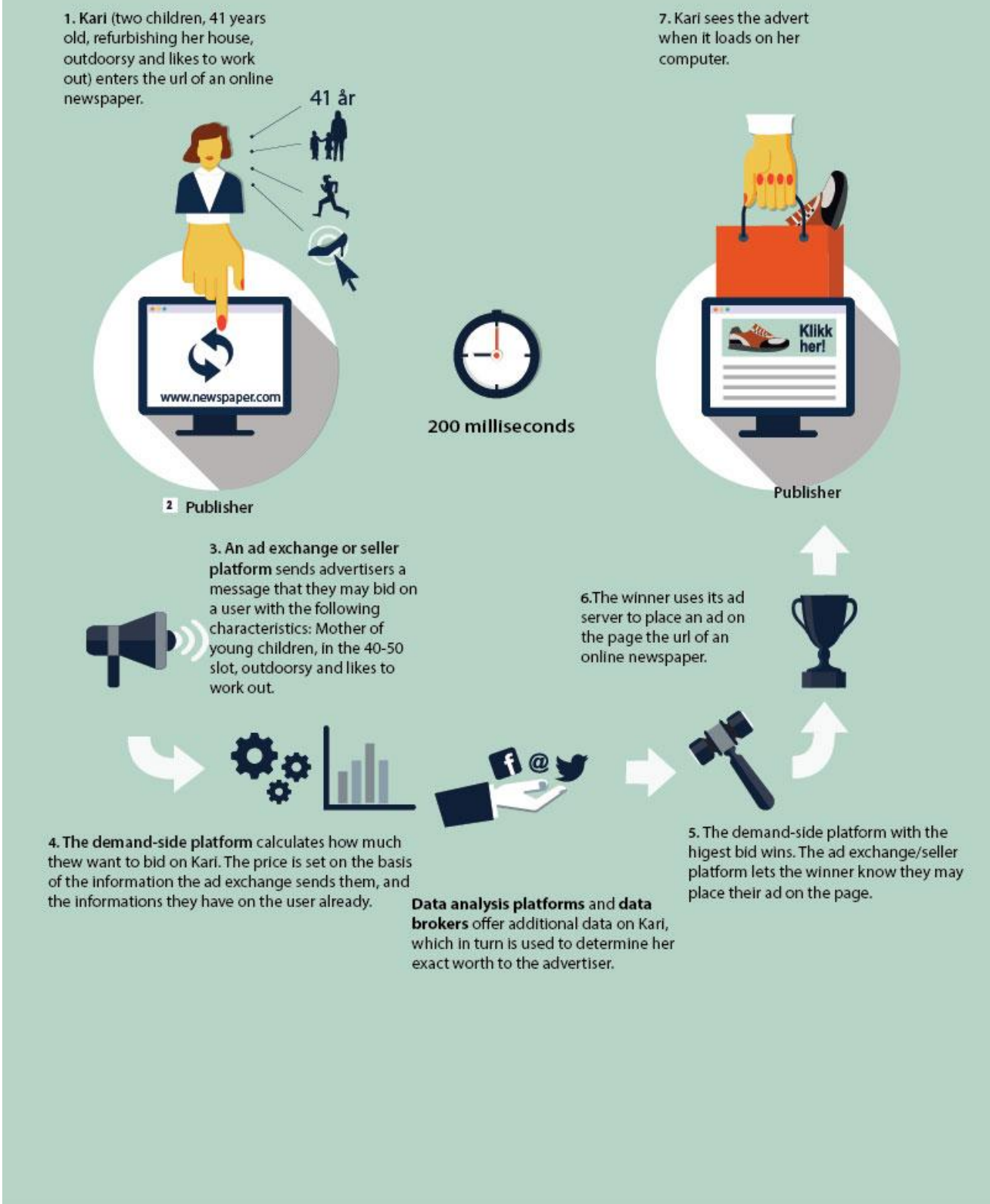
9 Le Monde Diplomatique, «Reklamerevolusjonen» [«The advertising revolution»], November 2013, http://www.lmd.no/?p=13010

10 Business Insider, «Google Is Now Bigger Than Both The Magazine And Newspaper Industries», 12.11.2013, http://www.businessinsider.com/google-is-bigger-than-all-magazines-and-newspapers-combined-2013-11

11 Dagens Næringsliv, «Kjemper om reklamebørs» [«Fighting over ad exchange»], 01.05.2015,

12 In the United Kingdom The Guardian has taken an initiative similar to Schibsted's. Along with CNN International, the Financial Times, Reuters and The Economist, The Guardian has set up the private market place The Pangaea Alliance. The initiators say sharing data is an important part of the partnership, ref: http://advertising.theguardian.com/pangaea-alliance/

Programmatic buying of users on ad exchanges



Another key strategy for media companies is developing solutions for targeting content, which goes hand in hand with targeted advertising. In order to increase the value of their ad spots, media companies can tempt advertisers with the possibility of displaying advertising for slalom skis to users beside content that reflects this interest.

Buyers of advertising space

The **advertisers** depend on publishers to market their products to potential buyers. Many advertisers possess large volumes of customer data, collected by means of loyalty cards or by other means. It is common for advertisers to use a media agency to assists them in placing advertising in the optimum manner.

Five large **media agencies** dominate the sector both internationally and in Norway: Public Omnicom Group, Denstu/Aegis, WPP, Interpublic Group (IPG) and Havas Group. In order to meet the competition from Google, Facebook, Microsoft and Yahoo, the media agencies are becoming technology companies with strong knowledge about data analysis, profile building and data harvesting. All the large media agencies have made several strategic acquisitions of large technology and data analysis companies in recent years.

The media agencies have one advantage compared to Facebook and Google, which is that they have access to customer data from their customers in the advertising industry. Customer data are valuable because they contain actual information about the customers and which products the customers purchased and find interesting. This is crucial data when creating targeted ads. The global head of research in Starcom (Public Omnicom Group) has said that the media agencies should become experts on administering data across businesses. Kjell Gabrielsen, manager of Xaxis (WPP's demand side platform) has said the following:

«We collect and process the data through our DMP (data management platform) in order to buy ad views only from the people the advertiser want to reach. (...) The data that Xaxis processes arrive from several sources. We buy third party data; demographic variables bought from external actors, second-party data; typically interests data based on experiences from previous purchases and first-party data; data straight from the customers. Data received straight from the customers are never used across customers.»

Advertisers wanting to buy ad space via an ad exchange must use a demand-side platform. **Demand-side platforms are** types of software that serve ads on behalf of the advertiser in real-time based on specified rules. The demand side platforms are most often operated by media agencies through a so-called *trading desk*, but there are also independent demand side platforms. Advertisers who do not wish to use a media agency can use Google's DoubleClick Bid Manager or other independent demand side platforms such as MediaMath or Rocktfuel.

The demand-side platform purchases users based on targeting criteria, an algorithm developed in partnership with the customer (the advertiser). The algorithm is based on aligning data from several different sources: customer data which the advertiser possesses, behavioural data collected by the demand side platform with the aid of cookies , and data collected from third parties, for example information collected from social media. When an ad exchange auctions a user who meets the criteria in the algorithm, the demand side platform will automatically decide the value of the user and submit a bid on behalf of the advertiser. The technology used is called cookie-matching. In order for the buyers to decide whether they want to make an offer and how much they want to offer, they need to know who the user is. Cookie-matching facilitates this (more on cookie-matching on page 20).

The demand side platform who wins the bidding round, will place a cookie in the user's browser when they show the ad. In this way they can measure how efficient the targeting algorithm is. If the user does not respond to the ad, the criteria for the algorithm are adjusted to avoid buying the same kind of user profile again. The placement of the cookies is also used to monitor the same user over time in order to reach the same person with corresponding advertising on other web sites, and to build up a user profile on that person.

Data management platforms, data brokers and market analysis

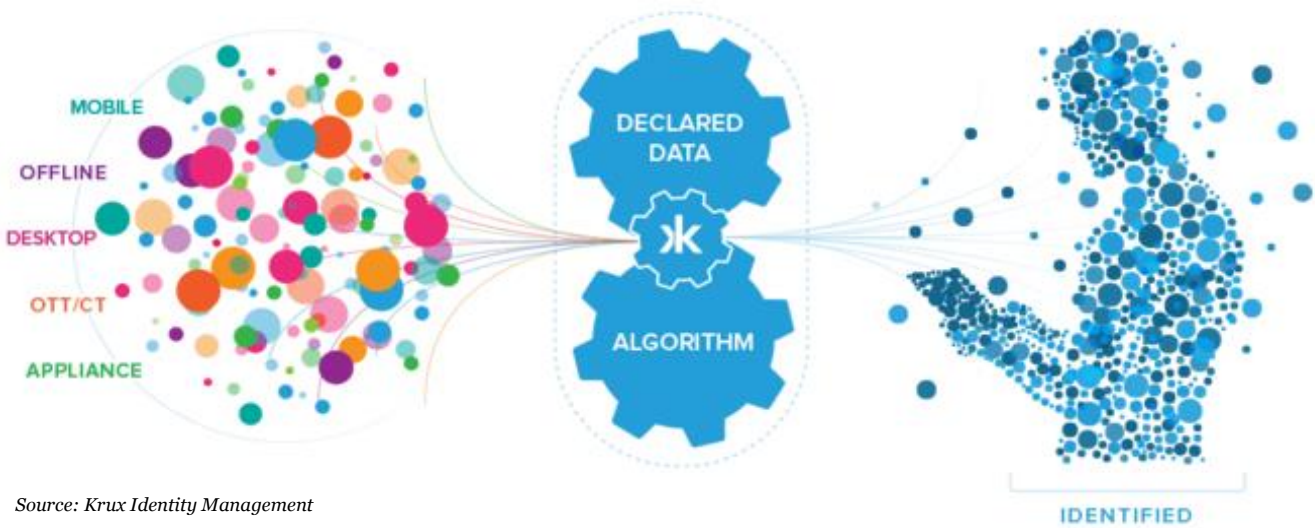
The fourth and last group of companies in the ad tech ecosystem is made up of companies who make a living from selling user profiles and data and market analysis to advertisers and publicists. As we will cover in chapter four, these companies make up the largest group of third-party players acting on a given website.

Data brokers are companies that collect consumers' personal data and resell or share that information with others. Because these companies generally never interact with consumers, consumers are often unaware

of their existence, much less the variety of practices in which they engage. [13] The Federal Trade Commission in the USA has published an extensive report that shed light on the data broker industry and its practices.

The biggest data brokers are American and include companies such as Acxiom, Experian and Datalogix. Even though the companies operate from the USA, they collect personal data from consumers regardless of national borders. Personal data is collected from a wide range of commercial, government, and other publicly available sourses, e.g. from social media. Data brokers also collect personal data from consumers by placing cookies on their browser. Data brokers infer consumer interests from the data they collect. They use those interests, along with other information, to place consumers in categories, such as «sports car owner» and «urban and eco-friendly» (more on building profiles in chapter four).

The **data brokers** hold a vast array of information on individual consumers. Acxiom, for instance, has information about 700 million consumers worldwide with over 3000 data segments for nearly every consumer.[14] Acxiom now has offices around the world, including in Europe.[15] Experian and Bisnode are examples of data brokers in the Norwegian market. As far as the Norwegian Data Protection Authority knows, these companies build up target groups and user profiles based on address lists, and aggregated and anonymous data collected from public registers and publicly available statistics. To our knowledge, these companies do not collect personal data through by means of cookies, for instance. However, because of international competition, data broker companies established in Norway and Europe will most likely look into the possibility of collecting and combining information from a wider array of sources than today.



Source: Krux Identity Management

[13] Definition taken from Federal Trade Commission, «Data Brokers. A Call for Transparency and Accountability», 2014, https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

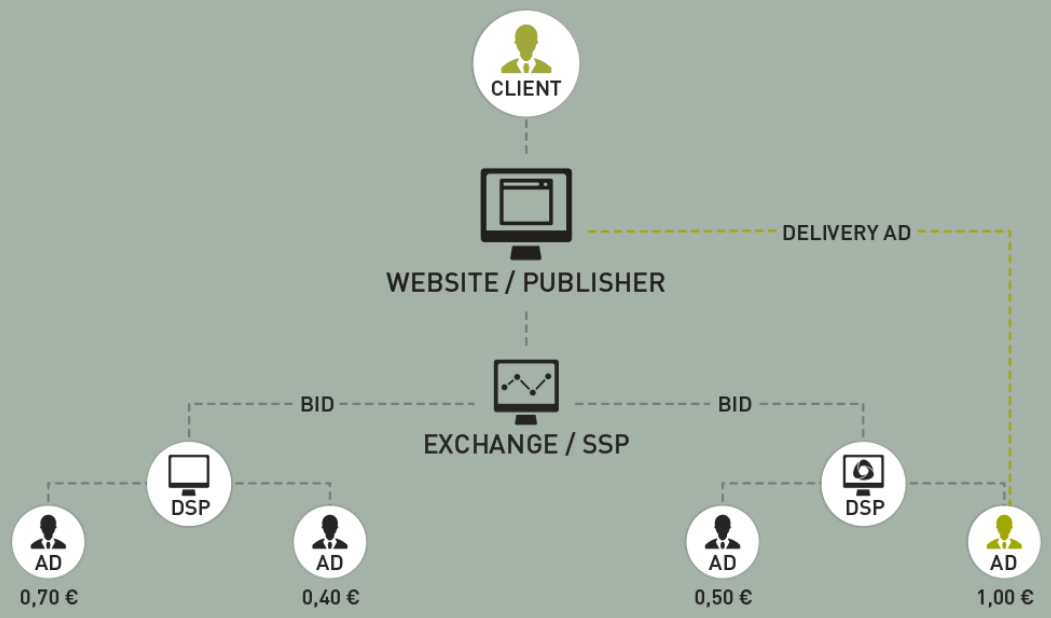
[14] Ibid.

[15] Acxiom has assisted the British media company The Guardian with identifying and integrating 75 different sources of customer data which are to be used to offer advertisers the most targeted advertising possible, ref: Acxiom, «Case study: The Guardian, Boosting audience engagement across the globe», 2014, http://dq2qu0j6xxb34.cloudfront.net/wp-content/uploads/2014/02/The-Guardian.pdf

A growing number of companies are now positioning themselves as demand-side platforms with integrated data management functionality, sometimes referred to as *consolidated media buyer platforms*. Acxiom, eXelate, Datalogix, Demdex, Epsilon, Experian, Digital, Lotame and Mediamath are companies that offer both functionalities. This means that they offer both tools to analyse data and to buy ad space. By integrating both functionalitites in one company they can harvest even more personal data from users online. Demand side platforms have, as previously mentioned, the capability to collect personal data from users in connection with the bidding process at the ad exchange and by placing cookies together with the ads. Data collected by the demand side platform can be feeded into the data management platform and used to develop ad-targeting algorithms.

Market research companies have traditionally been important to advertisers and media agencies during advertising campaigns. They contribute by finding the right target group and evaluating the effect of the campaign. The market research companies have mainly gathered data by using telephone interviews or web panels. The transition to real-time purchasing of adverts makes it necessary to be able to evaluate the effect of the targeting in real time, so that the targeting criteria can be continually adjusted if it turns out that they do not work optimally. In order not to be ousted by media agencies and other players providing data analysis, the market research sector is forced to develop solutions that make real-time analysis possible. That means deploying tracking methods that can monitor user behaviour in real time.

Real-time bidding, step by step



1. You sit down in front of your computer to read the news. You enter the address of the news site you want to view in the search field at the top of the page. For example www.newspaper.com

2. When you press enter, the web browser immediately sends a message to the data server of the newspaper, letting it know which page you wish to look at. This message is called a *get request* and consists of an HTML code.

3. Newspaper.com sends a code back to your computer that sets up the editorial content of the page you want to look at.

4. Newspaper.com also sends a code called *ad tag* with the editorial content. This code is linked to the adverts that will also be on the page. When this code reaches your computer, it immediately sends a notification to the ad exchange with whichnewspaper.com has an agreement. This notification, which is sent from paper's server to the ad exchange via your web browser, is called an *ad call*. The ad call notifies the ad exchange that the empty advertising spaces on the website you are accessing must be loaded with adverts.

5. The ad call lets the ad exchange know that it must conduct an auction to fill the advertising spaces with adverts. This notification also arranges for the exchange to have *access to you*.

6. The exchange now has the opportunity to read the cookies that it has previously installed on your browser (if you have not deleted them). These cookies were placed there when they last shown you advertising. The cookies enables the ad exchange to recognise you as a user who already has a profile. The exchange has set up a unique code for you on its server. Your unique code may for example be ABCD. By using cookies that the exchange has installed on your computer, it has accumulated data that make up a profile of you. The profile contains for example information about which adverts you have seen previously, which websites you have visited, technical information about your computer (type of machine, web browser, software and so on), IP address, location data. The code does not contain your name or other information that is directly identifiable.

Real-time buying continued

7. The exchange sends this unique code to all the demand side platforms that are linked to the exchange. This is also called an ad call. The ad call notifies potential bidders that they have the opportunity to send advertising to user ABCD with the characteristics contained in your profile. When the demand side platforms receive the ad call, this notification makes it possible for them to retrieve any cookies that *they* have placed on your computer during previous exchange transactions in which they have been allowed to show you adverts. If you have deleted these cookies, you appear to be a user with whom they have not previously been in contact.

8. The demand side platforms that wish to take part in the bidding round now try to find out as much as possible about you in order to decide how high a bid they will submit. They combine information collected from the cookies on your web browser with data collected from other sources, for example customer data supplied by the advertiser. The cookies provide information about how often they have advertised to you previously, what adverts you have been shown and the types of websites you have visited (they know which websites you have visited because they have information about which websites the advert you have been shown previously has appeared on).

9. All the various demand side platforms which participate in the bidding have profiled you. They do not know your name, but they know a great deal about your interests and shopping habits, and the profile becomes increasingly detailed as new information about you is gathered. Your profile has a unique code, for example 1234. The demand side platform also know one other thing: They know that the user they know as 1234 is the same user the exchange identifies as ABCD. Because they know that user 1234 and user ABCD are the same user, they are in a position to assess *how much* you are worth. The technique of linking the two user identities is called «cookie-matching» and is a crucial mechanism in the system of real-time purchasing.

10. All demand side platforms that assess participation in the auction perform a cookie match. By performing a cookie-match they are in a position to decide how much they are willing to bid on you specifically. If your profile shows that you still surf for luxury cars and that you have repeatedly bought expensive watches and jewellery, the DSP has developed an algorithm that will automatically submit a bid for you so that they can show you advertising for exclusive property or luxury cruises.

11. All the bidders state the figure they will pay for the right to show you adverts.

12. The auction takes place in real time. Real-time auctions are so-called second-price auctions. This means that the participants only submit one bid and that the bidder with the highest bid wins.

13. The exchange sends a notification to the demand side platform that won the auction.

14. The demand side platform that won sends a code to set up the advert in your web browser. This places a cookie on your machine at the same time so that it can recognise you at the next crossroads, thus accumulating more data for your profile.

15. The advert is displayed on the website just as the site is loaded on your screen. You are most likely completely unaware of all the players and all the processes that have been involved in this process, which has taken just under a millisecond.

** This description is taken from Smith, Mike, «Targeted. How Technology Is Revolutionizing Advertising and the Way Companies Reach Consumers», Amacom, 2015*

Collection of data

Many people believe that ad-funded content on the Internet is free. This is wrong. We pay for access to the services with our personal data. Personalised content and marketing requires an extensive collection of personal data. The word *relevance* is frequently used by the media and advertising industry. The more data are gathered about the individual, the easier it is to show users relevant advertising and content. All the players in the ad tech value chain collect personal data. This data collection mainly takes place out of sight.

In this chapter, we will first review the various techniques which are used to gather information about the user. We will then investigate which players are present and gather information about Norwegian users from a selection of Norwegian online newspapers.

Various types of tracking technology

Cookies, IP address, web beacons and device fingerprints

An advert for a washing machine appears on all the websites you visit after you have checked the prices of other models. This is a sign that you are being tracked by means of cookies[16]. The use of cookies is the most widespread technology for tracking users on the Internet. A cookie is a small file sent from a website and stored in the user's web browser while the user is browsing that particular website. Every time the user visits the website, the web browser sends information back to the website's server, notifying the website about the user's activity on the page. Companies can place cookies that are stored on people's computers for several years, even for more than 10 years, or use cookies which are immediately deleted when the web session finishes.

We can distinguish between so-called first-party cookies and third-party cookies. First-party cookies are small files that are distributed and controlled by website owners themselves. Third-party cookies are small files which website owners have put on their web page, but which are controlled by companies other than the website owner themselves. [17] Third-party cookies are principally placed by companies who work in market analysis and targeted marketing. Companies that are present through third-party cookies are usually not just present on one website, but on hundreds of websites. This makes it possible for companies to follow the same user from website to website and to build up comprehensive profiles of the person concerned on the basis of their browsing history.

From the advertising industry's perspective the use of cookies has several weaknesses: First of all, cookies are not suitable for tracking the same user *across* the user's various platforms (mobile, tablet, computer). Secondly, the use of cookies requires the consent of the user. Thirdly, it is possible for the end user to prevent the installation of cookies, and to delete cookies. Finally, cookies yield inaccurate data. Information collected using cookies does not yield factual information about real individuals. By analysing information collected by cookies, companies may make inferences about the user, for instance gender or age. The collection of personal data using applications or other solutions that require login yields more accurate data. Google has announced that in future it may stop using cookies.[18]

Web users can also be tracked by collecting their *IP addresses*. An IP address is a unique identifier that relates to a unit, such as a PC or a tablet, in a network such as the Internet. The IP address can provide information about the location of the user and which network it comes from. Most users have the same IP address for a certain period of time, and it can therefore be used to follow a user over that time. It is however not very suitable for tracking end users over a longer period in the way cookies enable you to do. The benefit of an IP address is that it is so accessible. The IP address is first retrieved by the website owner. Third parties who are present on the website can retrieve the IP addresses of users by using web beacons.[19]

16 We primarily use the term «cookies» and occasionally the expression «information capsules», both of which commonly occur in Norwegian. The terms are completely synonymous. See glossary p. 65 for more.

17 Third parties place cookies on the web browsers of the website's users by first placing a web beacon on the page. It is the website owner who lets third parties place these web beacons. The web beacon makes it possible for the company to retrieve the user's IP address. The IP address is needed in order to be able to place a cookie on the user's web browser.

18 USA Today, «Google may ditch 'cookies' as online ad tracker», 17.09.2013

19 An IP address can be indirectly linked to someone, and IP addresses are therefore treated as personal data in line with European privacy legislation. In the USA, however, IP addresses are not considered to be personal data and the American advertising industry is therefore much freer to use an IP address for profiling purposes.

Web beacons are used on their own or in combination with cookies to obtain more information about the visitors to a website. A web beacon is usually an invisible graphic image (normally 1 pixel x 1 pixel) which is placed on the website. Web beacons are also used by third parties to collect information about users and as a mechanism for placing cookies. Web beacons can be used to collect information about the user's IP address, the time when the website was visited, which web browser the user has and so on.

Norwegian media with log-in solutions

- **Schibsted** gathers information about its users through the SPiD identity and payment system**. SPiD**was introduced in 2013 and has 2.3 million users.
- **Polaris Media** uses SPiD for its newspapers, including Adresseavisen.
- **Amedia** has introduced the log-in service Aid which the company uses across its 60 local newspapers plus 1881.no, Nettavisen, parts of Blogg.no and a number of niche pages. The company's advertising network covers 2.5 million users.

It is not possible to protect yourself against the use of web beacons. Even if you indicate in your web browser that you do not accept cookies, you will still be tracked by web beacons

In order to get around the weaknesses of IP addresses and cookies as tracking tools, the advertising industry has begun using device fingerprinting. A device fingerprint is the unique electronic fingerprint that every computer has when it is connected to the Internet. The IP address, along with information about the type of web browser, choice of language, differences in the electronics and similar details can together produce a unique fingerprint to be called a device fingerprint. The advertising industry views such fingerprints as an alternative to cookies. Unlike with cookies, with device fingerprinting the user cannot refuse. Device fingerprinting therefore represent a serious threat to the individual's privacy. The European Commission's advisory body on privacy issues, the Article 29 Group, has made a recommendation about device fingerprinting. The Article 29 Group concludes that the rules for cookies should also apply to device fingerprinting. This means that consent must be obtained before information about the user's device is collected. From the industry's perspective the disadvantage of device fingerprints, as for cookies, is that the technology is not suitable for tracking the user across platforms.

Unique ID – the tracking solution of the future

Because of the weaknesses of the tracking options we have described so far, the major Internet players have developed new tracking methods to follow the user on the Internet and mobiles. All the biggest Internet companies have gradually developed *log-in solutions* which can track the user's unique identity (name, address, telephone number). The use of login solutions yields more accurate user data, which therefore are more useful and valuable for the various players engaged in the behavioural advertising industry than data collected by cookies. Login solutions keep the user perpetually logged on, making it possible to follow him or her from platform to platform throughout the day.

Facebook was the first large company to introduce continuous login to collect user data. Other major players such as Google, Microsoft and Amazon have followed. In Norway, all three of the largest media companies - Schibsted, Polaris Media and Amedia - have introduced log-in solutions. By introducing these, the publishers aim to gain greater control over their own customer data, so they can catch up with those players who have taken the lead in the race to collect and utilise user data for profiling most extensively and effectively.

The transition to log-in solutions represents a threat to players who base their analyses on data collected by means of third-party cookies. If a few log-in solutions become dominant in the market, media agencies and data brokers such as Bluekai and eXelate will have access to fewer data. To be able to track unique users

across platforms, we know that the media agencies are planning to create their own log-in services.[20]

Another method for obtaining information about users is performing the required registrations via apps. Not only does this enable the companies to keep the user constantly logged in, it also enables them to use the application serial number for identification purposes. This does not make tracking across platforms possible if the user is not then identified by, say, a name or mobile number. From the advertiser's point of view, one disadvantage of app registration is that the users want to limit the number of apps.

Large companies such as Google, Apple and Microsoft offer advertisers the possibility of tracking users via *AD-ID*. By using this tracking option the advertisers can follow the same user from the web to apps. Microsoft had to endure criticism at the launch of Windows 10 when it became known that users were automatically assigned an AD-ID when they downloaded the new operating system.[21]

Apple's «Unique Device Identifier» (UDID), a unique identity assigned to every individual Apple product, was previously available to other companies who wanted to reach apple users. This is no longer the case. The identity is linked to Apple's «Identifier for advertisers» (IDFA). This is a unique string of characters that is assigned to every user who utilises an iOS unit. For example, when adverts are run on Apple's iAd advertising network, Apple will know who receives the advert and potentially link it back to everything the person did elsewhere in Apple's system. It is possible for the user to set Apple's Advertisement ID to zero. It is also possible to avoid targeted advertising by turning off the permission for customised advertising.

Google has a corresponding advert identifier. The user can turn off this tracking element and deselect targeted advertising in Google's Play apps.

Cookie matching as a data-harvesting technique

The underlying technology to exchange users' identification data between ad exchanges and buyers is cookie matching, which allows two different domains to match their cookies of the same user. Cookie matching is an integral part of Real Time Bidding. In order for buyers to be able to decide whether they want to submit a bid, and as importantly, how much they will bid, they must know who the user is. Cookie matching enables the possibility of linking the profiles of a single user in databases of two independent companies. 22 When a user is put up for sale the exchange gives the demand side platform access to data about that user. For example, Doubleclick puts user 1234 up for sale with associated user data that tells that the user has visited the websites pets.com and pinknews.co.uk. The demand side platform AppNexus executes cookie matching which shows that user 1234 is the same as user xys, for whom they already have a user profile. AppNexus knows that this user has visited foxnews.com and cnn.com. After implementing cookie-matching AppNexus has received further information about user xyz with which it can update the user profile. Researchers have revealed that Real Time Bidding can leak as much as 27 per cent of a user's web browsing history to a bidder involved in Ad Exchanges' auctions. 23 The process is inherently non-transparent, and this invisible leakage cannot be observed using current tracking measurement tools such as Ghostery, according to the researchers.

In other words, cookie matching does not only function as a method for being able to identify and estimate the correct value of a user in connection with Real Time Bidding. Researchers who have studied how cookie matching is used, claim that the technique is also used as a method for data harvesting in order to build up user profiles. [24] Google however, states in its user conditions that it does not permit cookie matching to be used for this purpose.[25] The Norwegian Data Protection Authority will take a closer look at the use of cookie matching in order to gain greater insight into how this technique functions and what purposes it is used for in connection with real-time bidding.

---

[20] Adweek, «Google's Latest Role: The Cookie Monster. Ad tech firms are on alert», 11.11.2013, http://www.adweek.com/news/technology/google-s-latest-role-cookie-monster-153712

21 TechRepublic, «Windows 10 violates your privacy by default, here's how you can protect yourself», 4.8.2015, http://www.techrepublic.com/article/windows-10-violates-your-privacy-by-default-heres-how-you-can-protect-yourself/

22 Olejnik, Lukasz, Tran Minh-Dung and Claude Castelluccia, «Selling Off Privacy at Auction", 2013, HAL Id: hal-00915249, https://hal.inria.fr/hal-00915249/PDF/SellingOffPrivacyAtAuction.pdf

23 Ibid.

24 Ibid.

25 https://developers.google.com/ad-exchange/rtb/cookie-guide

Beacons – linking analogue and digital worlds

Up until now, the advertising industry has had no way of linking people's activities in the real world to people's activities on the Internet. The use of beacons makes this possible. Beacons are small sensors using Bluetooth technology to send information that can be received when someone comes close to them. Using this technology requires that the user has a device that can read the information that is transmitted.[26] By placing beacons it is for example possible to register which products customers look at on shop shelves. This information can be picked up by an app in a smart phone, and can later be used to send the user targeted advertising for the product the person looked at in the shop. By linking beacons in a large network they can function as an offline cookie, tracking users as they move between shops, cinemas, museums, bars, restaurants and sports arenas.

Thomas Walle Jensen, Co-founder and CEO of Unacast, the world leader in the development of beacoms, says: «Retailers and brands have a limited customer view today. As soon as the customer leaves their store, he or she becomes invisible, until they resurface in the same location. What the customer did before and after the visit is unknown. By working with Unacast and sharing data into the Unacast PROX network, retailers and brands can ensure that in-store campaigns can take into account the total physical profile, thus fulfilling the promise of proximity as the offline cookie.»[27]

Vast presence of third parties

Every time we visit a website, we do not just engage with one company, but with many companies simultaneously. As well as the publisher who owns the site, ad exchanges, demand side and supply side platforms, data management platforms, data analytics companies and data brokers are present with various tracking tools in order to gather information about us. All the companies that are present, apart from the site owner, are who referred to as third-party players.

News websites can be seen as two separate entities:

The part controlled by the publisher: This part of the website consists of the journalistic content of the newspaper. Here the publisher determines which third-party players are allowed access and what personal data these players may collect. These third-party players often process personal data on behalf of the publisher and therefore have the status of data processors. These third party actors typically include data analysts, data management platforms, supply side platforms, ad exchanges and demand side platforms. Examples of companies used by Norwegian publishers are Cxense, Google Analytics, Google Doubleclick, AdForm, TNS, Rubicon and AppNexus.

The part controlled by the advertiser: This part of the website consists of the advertising space which are assigned to external players. This is where the advertisers are allowed in. The companies buying ad space, typically media agencies and the demand side platforms, are present on this part of the web site. The media agencies bring a number of companies onto the page with them to mesure and anlyse the effect of the ads they place and to trace users from one website to another. In a way these companies are the media agencies' third parties, or the third parties' third parties, if you will. The publisher has no control over the third-party players present in this part of the website. Examples of companies that are present her are Datalogix, Google Doubleclick, Facebook, Rocketfuel, The Trade Desk, Media Math and Dataxu.

«A site is not one company any more. A site is tens of hundreds of companies all knowing where you are and what you're looking at.»

Chris Babel, TRUSTe»[28]

Third parties on Norwegian online newspapers

We have studied which third-party players are present on six Norwegian online newspapers, and how many

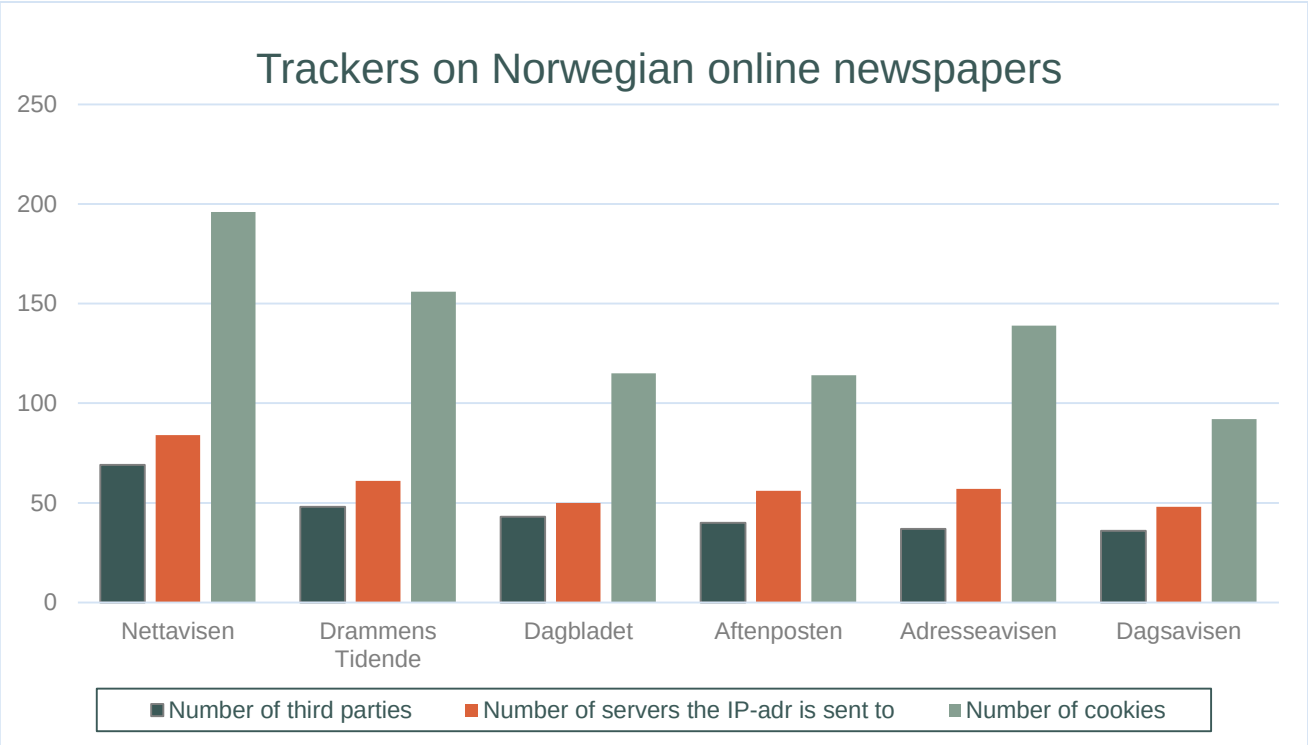
26 Google has however developed beacon technology which does not necessarily require the installation of an app. Google's Eddystone is an open beacon format. An Eddystone beacon signal can be received directly by apps or as an Eddystone URL which can be used by smart phones even though they do not have the company's app installed.

27 http://unacast.com/welcome-to-unacast-prox-network/

28 The Economist, "Little Brother, Special Report on Advertising and Technology", 13.09.2014, http://www.ogilvydo.com/wp-content/uploads/2014/09/20140913_SR_MAILOUT.pdf

cookies are placed on a web browser when visiting these sites. The newspapers we have studied are Aftenposten, Dagbladet, Nettavisen, Adresseavisen, Dagsavisen and Drammens Tidende.[29]

The conclusion of the study is that there is a massive presence of third party players. The number of cookies is also enourmous. Between 100 and 200 cookies were placed on our browser when we visited the papers' front pages. Our IP address was sent on to 356 servers. On average 46 third-party players were present on each of the six Internet newspapers we studied. In total 11 ad exchanges, 12 demand side and supply side platforms, 12 data management platforms, 8 data brokers and 13 data analytics companies collected information about us (see appendix 2). The great majority of the trackers are American companies. Only a few are European, for example cXense (Norwegian), Internet Billboard (Czech), Semasio (German) and Adscale (German).



The newspaper with most third-party players present is Nettavisen, where at least 69 different companies were present. With the help of web beacons these companies send our IP address to 84 different servers. The same companies also place 198 cookies on the web browser. Drammens Tidende also has many third-party players present on its site. A total of 48 companies send our IP address to 61 servers and place 156 cookies. The number of third-party players and the amount of cookies that are placed has exploded in recent years. The transition to programmatic trading is probably the cause of this growth.

Information deficit

None of the six newspapers give the public information about the presence of third-party players on their pages. The privacy policies only provide general and vague information about the use of cookies.

29 The study was conducted on 4 September and 7 September 2015. We accessed the front page of each of the six newspapers. We used the Ghostery analysis tool to obtain information about the number of third-party players and the number of tracking elements which were placed on our web browser when visiting the sites. We chose newspapers from all the three major Norwegian newspaper publishers (Schibsted, Amedia and Polaris Media), a national newspaper (Dagbladet), a regional newspaper (Aftenposten) and a local newspaper (Drammens Tidende). We also picked out a newspaper which is exclusively an Internet publication (Nettavisen).

Google's global dominance

Google is present on 87 per cent of all Norwegian online newspapers (trackography.org). Google has made the greatest progress on gathering information about us as individuals. Google uses many different services and technologies to gather information about users:

- DoubleClick
- Google Analytics
- Google tag manager
- Google search
- Google Gmail
- Google maps
- Google Street View
- AdSense
- AdWords
- YouTube

Google gathers information about individuals both directly and indirectly. The company gathers information direct from users through services such as Gmail, search, YouTube and maps, and indirectly as a third-party player (on millions of websites around the world) via services such as DoubleClick, Analytics, AdSense and AdWords.

The Norwegian Communications Authority conducted an inspection of the cookie provisions in 2015.[30] The inspection revealed that only 19 per cent of the 500 websites investigated complied with the provisions. The media companies were the worst of all. Fully 9 out of 10 news sites do not meet the law's information requirements.[31]

Why do not website owners provide more detailed information about the third parties present on their sites? Are they worried that if we knew what was going on behind the scenes, we would ask critical questions or refuse to use their services?

As has been stated, one explanation may be that they do not have a complete overview nor control over which companies are present in those parts of the web service that have been allocated to ad spots. Some publishers therefore leave it to the user to avoid being tracked by providing information that users can adjust settings on their machine so that cookies are not placed in the web browser. However, using this setting only helps against some of the tracking. Even though the users have protected themselves against cookies in their web browser, third-party players can follow them by using other tracking tools we have discussed.

Being tracked on the Internet is not something you opt into. The default is almost always that you are tracked. If you want to opt out of tracking there are rarely good mechanisms in place to allow you to do this. The Internet Advertising Bureau (IAB) has set up the Youronlinechoices.eu site, where users can ask companies to stop tracking them with cookies. Here users can click on the companies they want or do not want to follow them, or click on the green button to "switch on all companies" or the red one to "switch off all companies". It is however only the most privacy-conscious consumers who will seek out this service in order to opt out. Most consumers have no idea that they are being tracked and will use online services in their default mode.

30 The Norwegian Communications Authority is an autonomous agency of the Norwegian Ministry of Transport and Communications and inspects and monitors providers of postal and telecommunications services.

31 The Norwegian Communications Authority, «Tilsynsrapport. Tilsyn etter Lov om elektronisk kommunikasjon § 2-7 b. Bruk av informationskapsler/cookies» [«Inspection report. Inspection according to the Norwegian Electronic Communications Act»], 2015,

Building profiles

Advertisers and publishers use the information collected with the help various tracking technologies to develop user profiles. The profiles form the basis for personalising content and adverts. In this chapter we will look at what information the profiles contain and how much they are worth.

What is a profile?

A profile is made up of *assumptions* about the preferences, abilities or needs of an individual or a group of individuals. The inferences are made from analysis of individuals' browsing history, updates on social media, which news articles they read, products bought on the Internet and registered customer information. Nowadays profiling is to a great extent about using Big Data analysis to look for patterns and connections in large data sets which can be used to predict consumer behaviour.

According to the European Data Protection Directive, inferences are also to be regarded as personal data, even though they do not strictly make up factual information.

The use of profiles as *the basis for making decisions about an individual,* is of key importance from a data protection perspective. It is a fundamental privacy principle that decisions about an individual should be made on the basis of accurate data. Hence, it is of great importance that the individual has access to the information which is collected about him- or herself. This allows the person to review whether the information is accurate. This goes some way to ensure that incorrect decisions based on the information is not made. Today, we have user profiles that were created without our knowledge and consent, by companies whose existence we are unaware of. This makes it challenging for the individual to protect their privacy. We will discuss this further in chapter seven.

Profile building is not a process which has a beginning and an end, it is a continuous activity. All the players in the value chain - the advertisers, media agencies, ad exchanges, data providers and publishers, *constantly update our profiles with new data* collected from our analogue and digital lives. We have no insight into how long the major Internet players such as Google, Yahoo! and Microsoft store our data nor how comprehensive our personal profiles gradually become. Presumably the volume of information is enormous. A study conducted by a Norwegian business daily (Dagens Næringsliv) showed that in the course of a year the Norwegian media company Schibsted had recorded 136,000 data points about a single user. [32]

«We now have a stalker economy where customers become products.»

Al Gore[33]

The actors in the field differ in their **motivations** for creating user profiles:

- Advertisers create profiles to distinguish attractive customers from less attractive customers so that the advert becomes as effective as possible.
- Publishers create profiles in order to attract advertisers to their ad spots. The more detailed and comprehensive user profiles they offer on the ad exchanges the more money advertisers are willing to pay.
- Data brokers harvest information and create profiles which they sell to both advertisers and publishers who want to enrich their own profiles with additional information.

Many advertisers and publishers claim that the user profiles they accumulate only contain anonymous data . This may be correct in the context of American legislation, in which only *directly identifying* information is regarded as personal data. American companies can for example store IP addresses in user profiles without this being regarded as personal data. Removing information such as names, addresses and e-mail addresses is sufficient. European privacy legislation does not view such profiles as anonymous in the same way. In European legislation *indirectly identifying* information is also defined as personal data.

[32] Dagens Næringsliv, «Dette vet mediekjempene om oss» [«The media giants know this about us»], 19.10.2014,

[33] Pando, «Al Gore says Silicon Valley is a 'stalker economy'«, 11.06.2014, https://pando.com/2014/06/11/al-gore-says-silicon-valley-is-a-stalker-economy/

This applies for example to IP addresses or data collected with the help of cookies.

Many in the Norwegian industry also claim that they only use anonymous data for profiling and segmenting users. It has not been possible for the Norwegian Data Protection Authority to ascertain the extent to which this is actually the case. It is however our impression that many companies believe that pseudonymous data are the same as anonymous data. Pseudonymous data still contain identifying information, even though names and addresses have been removed, and is therefore still regarded as personal data. There is further comment on this in chapter 6.

The content of the profiles

A user profile is made up of data which tells as much as possible about the individual. The more data are found in a profile, the higher value it has in the market. As shall become evident, the value depends on *what* information is found in the profile.

As has been mentioned, the profile does not necessarily contain directly identifying indicators such as name, address and e-mail address, but the information is linked to a unique number which makes it possible to follow the same user over time, thus gradually enriching the profile with new information as it is accumulated.

The actors in the field create the profiles in more or less the same way, with some fixed content categories. A user profile is usually made up of the following data categories:[34]

- **Demographic data:** This is background information about the user. This may be information about name, address, gender, age, marital status, post code, level of education, employment (type of sector), income, the number of family members in the household, number of children, age of children, property ownership, which car they own, ethnicity, religious affiliation. Demographic data are often collected in association with users registering in order to use new services. Demographic data can also be deduced from cookie data or from updates on social media. It is also normal to use statistical data to accumulate a broad set of background variables about individual users. For example, presumed party affiliation is linked to a user profile based on the post code of the person concerned.

- **Location data:** This is information which reveals where the user is located, collected via GPS, Wi-Fi and their IP address. Information about user location is very useful for advertisers in targeting adverts. For example, it is useful to know which users live in a place where it rains at a given time if they wish to target advertising for umbrellas and rainwear.

- **Technical data:** This is information linked to the user's computer, smart phone, tablet and possibly other devices which connect to the Internet. Examples of technical information are IP address, operating system (such as Windows 7), web browser (for example Internet Explorer 10) and screen resolution.[35] From technical data, in

[34] Rao, A., F. Schaub and N. Sadeh, «What do they know about me? Contents and concerns of Online Behavioral Profiles», Carnegie Mellon University, 2014, https://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab14011.pdf and IAB Europe, «Programmatic Trading. An IAB Europe White Paper», 2014, http://www.iabeurope.eu/files/8614/0776/0957/IAB_Europe_Programmatic_Trading_White_Paper_July_2014_v2.pdf

[35] Rao, A., F. Schaub and N. Sadeh, «What do they know about me? Contents and concerns of Online Behavioral Profiles», Carnegie Mellon University, 2014,

Companies which build user profiles operating in the Norwegian market

eXelate – owned by Oracle and one of the world's largest companies in gathering and analysing third-party data. The company says it gathers user data about 200 million unique users a month by being present with cookies on hundreds of websites. eXelate tracks unique users in order to see who is looking for a new car or is preoccupied by sports equipment.

BlueKai, a competitor of eXelate, claims it has profiles of 700 million unique users. They predict what types of purchases it is likely that the users will make on the basis of information about web behaviour.

Schibsted - the company gathers information about its customers' reading habits via its log-in solution, which comprises several newspapers and finn.no. It can use this knowledge to deduce further information about the user, for example about interests and hobbies. The newspapers also have demographic data about the reader, such as the user's gender, age and address. All of these are valuable data to offer advertisers who want to reach very specific target groups.

particular the IP address, it is possible to deduce a lot of other information about the user such as name, postal address, mobile number and history of buying goods on the Internet. Technical data are also used to assess users' purchasing power.

It has been revealed that Mac users who make purchases on travel websites pay more per night for hotel rooms than PC users.[36]

- **Interests data[37]:** This is information about the user's interests and attitudes. The information is usually deduced from analysis of data collected with the help of cookies which show which websites and adverts the user has visited in the span of weeks, months or years. Analysis of search and browsing history produces a rich image of the individual. It may for example reveal an interest in health or slimming products (search for sleep problems, pain, diets), interiors, travel (booked a hotel on Majorca and long weekend in Paris) and politics (clicked like on a Facebook post by Norwegian Labour Party leader Jonas Gahr Støre).

- **Predictive data:** Analyses are performed to calculate the probability of the user buying specific products on the basis of all the information which is collected. The predictions are made by analysing large volumes of aggregated data, but the result of the analysis is linked to individual user profiles. One example of a technique which is used to build profiles is twin analysis: The probability of an individual behaving in a specific way can be predicted on the basis of previous behaviour. This prediction can be transferred to other individuals who share the same characteristics. An example of predictive data found in one and the same profile is: "personal health: 70-90 per cent", which indicates the probability of the person concerned purchasing health-related products in the near future, "domestic flights – 70-90 per cent", which indicates the probability that the person will buy airline tickets, and "car insurance on the Internet – 16-17 per cent", which indicates the probability of the user buying car insurance on the Internet soon.[38]

- **Behaviour:** This is information about the user's lifestyle and personality. The users are segmented into various categories based on analysis of aggregated data collected by using cookies, social media, customer records, purchasing history and so on. The users are assigned labels which indicate their consumption patterns and purchasing power, for example "active lifestyle and SUV", "home-made food", "children first" and "urban, single and low

[36] Washington Post, «On Orbitz, Mac Users Steered to Pricier Hotels», 23.08.2012, http://www.wsj.com/articles/SB10001424052702304458604577488822667325882

[37] In English this group of data is called *psychographic data*

[38] Rao, A., F. Schaub and N. Sadeh, «What do they know about me? Contents and concerns of Online Behavioral Profiles», Carnegie Mellon University, 2014,

consumption". [39] There are also companies that use information collected to predict people's personalities based on Myers-Briggs personality type indicators (extrovert, introvert, leader, communicator and so on). The V12 company sells user profiles to advertisers and claims to have assigned a personality type to 85 per cent of all consumers in the USA, based on Myers-Briggs' different types.[40]

- **Life events**: This is information about important events that affect people's purchasing patterns, for example pregnancy, recent marriage, leaving home, moving house, and so on. Such information is often deduced from analysis of Internet behaviour. Browsing history shows for example that the user has read tests of buggies and articles about health and pregnancy.

What is a profile worth?

Do you think the advertisers will pay 10 Euro or 1 Euro for your browsing history? The system of real time bidding allows us to discover just how much a profile is worth. Researchers have revealed that advertisers pay more for users with a known browsing history, that is users who have cookies installed in their web browser and whom the advertisers thus already are familiar with, than users who are new to advertising buyers, for example because they have deleted cookies from their web browser.[41] Advertisers pay the most for users for whom they can re-target adverts. This is the instances where advertisers push adverts for shoes to a user whom they know has been looking at shoes or been exposed to advertising for shoes on another website.

The researchers found that the price can be as much as two to three times higher for user profiles which permit retargeting. The study also showed that not only their browsing history, but also which types of pages the user visits affects the price. Advertisers pay more for users who visit news sites such as Fox News than websites about combat sports, for example. Correspondingly, online shopping and looking at cars are types of behaviour that produces higher prices than browsing on sports sites. The study also revealed that users geographically located in the USA had a higher value than users in Europe.

In isolation, the price obtained for a profile is not particularly high. According to the researchers behind the study referred to above, the average winning bid on a user, is **0.00043 euros**. The "How much is your data worth?" project conducted under the auspices of The Financial Times identified the same figure. In the latter project it also emerged that some life events contribute to increasing the price advertisers are willing to pay for a user. Higher bids were submitted for profiles that showed that the user had just given birth, moved house or got divorced. Access to information about a woman who is seven months pregnant results in prices 240 times higher than the average price..

The more intimate and sensitive the information the advertiser has access to, for example information about health or consumption of certain pharmaceuticals, the higher the price advertisers are willing to pay. Information about the use of pharmaceuticals is sold for two Norwegian kroner per person, which is 22 European cents or 23 American ones, according to The Financial Times.[42] From a privacy perspective, it is unfortunate if this great willingness to pay for sensitive information stimulates more extensive collecting and sale of such information.

39 Turow, Joseph, "The Daily You. How the New Advertising Industry Is Defining Your Identity and Your Worth", Yale University Press, New Haven and London, 2011.

40 Bizreport, "Platform creates customer profiles using Myers Briggs types", 19.04.2012, http://www.bizreport.com/2012/04/platform-creates-customer-profiles-using-myers-briggs-types.html

41 Olejnik, Lukasz, Tran Minh-Dung and Claude Castelluccia, «Selling Off Privacy at Auction», 2013, HAL Id: hal-00915249.

42 The Financial Times, «How much is your personal data worth?», 12.06.2013.

What is the legal picture?

We have seen an explosive growth in the number of transactions in which personal data are traded to make marketing more targeted.
In this chapter, we will take a closer look at the legal framework for these transactions.

The Norwegian Personal Data Act

The Norwegian Personal Data Act regulates the processing of personal data. This is a general act, which applies to both the private and public sector. It came into being as a result of the EU's Data Protection Directive, by which Norway is bound under the EEA Agreement.

The aim of the Norwegian Personal Data Act is «to protect the individual against their privacy being violated through the processing of personal data». The act is the legal framework to which those processing personal data must adhere.

When does the act apply?

The Norwegian Personal Data Act regulates the processing of personal data. In order for the act to apply in relation to behaviour-based or custom marketing on the Internet, the data that are processed must wholly or partially be personal data. The act defines personal data as «information and assessments that can be linked to an individual person».[43]

In principle, all conceivable information which can tell us something about someone is covered by the term. In a world which is network connected, this covers much of the information which is amassed when we use the Internet; for instance which websites we visit, what we search for, and how we use the various services.

The salient point is whether the collected information is linked to an individual person so as to be considered personal data.

In assessing whether the person can be identified, one must consider the use of all tools which it is reasonable to believe that someone may use to identify the person. For example, the preparatory work for the Norwegian Personal Data Act states that «someone who records visits to their website gains access to an anonymous electronic identity which can only be linked to an identifiable individual person if you have access to information held by the person's Internet provider». Even this limited identification opportunity, however, is sufficient for the electronic tracks to be «personal data». [44]

In a statement from 2010, the Article 29 Working Party proclaimed that it is fundamental that data that are gathered and processed in relation to behaviour-based or custom marketing on the Internet must be regarded as personal data. [45] [46] This view is guided by the fact that behaviour-based marketing is normally based on gathering IP addresses or unique identifiers by means of cookies or other techniques. This allows companies to follow a user over time and to distinguish users from one another. The collected information tells them something about the person's characteristics and behaviour, and is used to influence the person through marketing. It must also be taken into consideration that at a given time the data can be linked to directly identifying information. This happens for example when user accounts are set up, or simply as a result of an ever-growing volume of data, which in itself can come to reveal the identity of the person in question.

The Norwegian Data Protection Authority shares this view. As long as the data that are collected are suitable for distinguishing users from each other they must be regarded as personal data. Behaviour-based marketing is organised in such a way that the individual user is recognised when he or she visits a website and

43 For a broader review of the term 'personal information' please see the Norwegian Data Protection Authority's Big Data report: http://www.datatilsynet.no/Nyheter/2013/Big-Data-rapporten/

44 Ot. Prp. Nr. 92 (1998-1999) page 101.

45 The Article 29 Working Party is a body which was set up pursuant to article 29 of the Privacy Directive. It issues interpretative statements with a view to harmonising the directive across the member states.

46 Opinion 2/2010.

marketing can be adapted. It must be based on the fact that it is possible to identify the individual user. The data and the people behind them are not anonymous.

The act's territorial scope

The act applies to a controller established in Norway.[47] In the context of the act "controller" means the legal person who decide the purpose of the processing of personal data and what methods are to be used[48]. In this report we often use the word company' rather than the term "controller" as it is generally companies who are behind the gathering and use of data for marketing purposes via the Internet.

The link between Norway and the company behind the processing of personal data is the crux of the matter. The company must be established in Norway for the act to apply. Being 'established' in this context means that the company responsible must conduct some form of activity in Norway of a relatively permanent nature. [49] The activity does not have to be conducted through a separate and independent legal person in Norway. The key consideration is whether the company has a sufficient link to Norway for it to be said to be established in the country in a general linguistic sense.

In light of the directive

According to the directive, it is not sufficient for the controller to be established in Norway – that is, conducting activities or business in Norway. Decisive here is whether og not the processing of the personal data in question takes place in the context of the company's activities in Norway. Thus there must be a natural link between being established in Norway and the processing of personal data for the act to apply. This must also be read into the Norwegian Personal Data Act.

In practice, it may be difficult to decide whether the organisation responsible for processing is established in Norway. An important example from case law is the so-called Google judgement, in which the Court of Justice of the European Union ruled that Google Inc., which is behind Google's search engine and operates it, must be regarded as being established in Spain. [50] What was decisive for the court was that Google has established a company in Spain – Google Spain. This company is responsible for selling and promoting Google's commercial marketing activities, including selling advertising space on the search engine's website. The court believed that the search engine and marketing activities is clearly connected. The search engine is operated commercially with a view to making money, including as a platform for adverts. Google Inc.'s operation of the search engine therefore has a clear link to Google Spain's activities and vice versa. The court subsequently ruled that when Google Inc. processes information about people in Spain through its search engine this happens in the context of the marketing activities Google conducts in that country. The company was therefore bound by the directive to comply with the Spanish Personal Data Act.

The Norwegian Data Protection Authority has said it is important that the same applies to Google in Norway, as Google has also established a company here, Google Norway AS. The purpose of this company is to generate sales of as well as marketing Internet advertising.

If the company is not established in Norway but in another EU/EEA country, then that country's laws apply to the processing of personal data.

If the company responsible for processing is not established in the EU/EEA area, it follows from the Norwegian Personal Data Act that the law applies anyway, if the company uses equipment in Norway for processing personal data. According to the preparatory work on this, the term 'equipment' is intended to cover all kinds of equipment that can be used to process personal data. [51] One important exception is however equipment which is merely used to transfer information via Norway – that is, purely carrying information through Norwegian networks.

Most people today use a mobile phone, PC or tablet for our internet-based activities. Much of this activity is recorded, saved and further processed with a view to profile building and custom marketing. How far the equipment criterion stretches here is uncertain. Statements in the preparatory work indicate that such devices must be regarded as equipment. The Article 29

47 cf. section 4 first paragraph first point.
48 See section 2 no. 4.
49 Ot.prp.nr. 92 (1998-1999) pages 105-106.
50 Pronounced by the Court of Justice of the European Union in case C-131/12.
51 Ot.prp. nr. 92 (1998-1999) page 106.

Working Party has also taken as its view that someone's PC is equipment in the sense of the directive[52].

The salient point for whether the act will apply is however that the company collecting the data some how make use of the person's PC, mobile phone or other in doing so. One example of this is when the company places a cookie on the person's PC. In that case, the equipment is used actively as part of the data collection. The Article 29 Working Party has argued that such utilisation of the equipment triggers application of the directive. Correspondingly, the Article 29 Working Party believes that using JavaScript or similar programs on the user's PC may mean that the equipment criterion has been fulfilled.

The extent to which the directive applies to companies which are not established within the EU/EEA has not been clarified through case law.

Legal basis for processing personal data for marketing purposes

The Norwegian Personal Data Act indicates various legal bases for processing personal data.[53] If sensitive personal data are to be processed it is also required that one of the legal bases in section 9 are present. [54]

A key question is whether the processing of personal data is conditional on the individual's consent , or whether processing can take place without consent. In principle consent must be acquired. There will however be exceptions where processing may be viewed as legitimate due to other legal grounds in the act.[55] There are two alternative legal bases for consent in the act which are of interest in this context, and which we will look at in more detail:

When the processing of personal data is required to fulfil an agreement

It may be claimed that the use of various internet-based services – for example social media – represents a form of mutual contract in which the individual gains access to and can use the service in exchange for being exposed to advertising.[56] As an extension of this, it may be argued that the processing of personal data in order to adapt the marketing to the individual is a necessary part of the contract. The individual then pays for the service indirectly with their personal data.

This view cannot be said to have had a significant impact. The Article 29 Working Party has for example clearly stated that the corresponding provision in article 7 (b) of the Data Protection Directive cannot be applied to profile building.[57] This must also apply where the purpose of profile building is to produce behaviour-based advertising. The key point is that such processing of personal data cannot be regarded as strictly necessary for providing the service. The fact that behaviour-based marketing is useful and profitable does not mean that the necessity requirement has been fulfilled.

The Balance Test

«Processing is necessary for the organisation responsible for processing to be able to pursue a legitimate interest, unless the data subject's privacy outweighs this interest.»[58]

This provision in the Norwegian Personal Data Act is often referred to as "the balance test'. The commercial interest which lies in operating custom marketing is legitimate and justified. However, private life considerations are assigned considerable weight when being balanced against commercial interests.[59] The processing must also be necessary. The necessity requirement means that the processing in question must be the least invasive approach in order to safeguard the commercial interest (subsidiarity), and that the processing must be proportionate overall.

The results of the assessment can vary from one instance to another. However, the general rule will be that the collection and analysis of data generated by individuals' use of Internet services for marketing purposes will come into conflict with the necessity requirement. It will also be overridden by the interest of

52 Working document on determining the international application of EU data protection law to personal data processing on the Internet of NON-EU based web sites.

53 Cf. section 8.

54 See the definition of sensitive personal data in section 2 point 8 of the act.

55 For a more broad-based review see Fredrik J. Zuiderveen Borgesius, Personal data processing for behavioral targeting: which legal basis?, International Data Privacy Law 2015 vol.5 no. 3.

56 cf. the Norwegian Personal Data Act section 8 a

57 Opinion 6/2014 page 17.

58 cf. the Norwegian Personal Data Act section 8 f.

59 See Ot.prp.nr. 92 (1998-1999) page 109.

privacy. This applies in particular in the case of tracking individuals across various services.

It is nevertheless possible to conceive of instances in which processing personal data can find its basis in the balance test: An Internet bookshop may collect information about the individual's behaviour on its own website only, for example which books are clicked on or purchased, in order to make recommendations. This is a form of marketing. The next time the person returns, this may be legitimate on the basis of the Norwegian Personal Data Act's section 8 f. However, the company must presumably still give the individual the opportunity to opt out.[60]

Consent

As we have seen, the legal person who collects and processes personal data in order to conduct behaviour-based marketing to the individual must base this on consent according to the Norwegian Personal Data Act.

Express consent is a *freely given, explicit and informed* statement by the data subject that he or she accepts the processing of information about themselves.[61] By premising permission to process personal data on consent, the individual is given the power and the opportunity to decide for him- or herself. In this way, the consent requirement arguably is at the core of the individual's right to privacy.

The requirement that consent must be freely given entails that there must not be any form of compulsion or pressure – it must be genuinely voluntary. If saying 'no' is to the disadvantage of the individual, this may represent a form of pressure that is incompatible with the requirement. If for example the real alternative to consent is to *not* use the service in question, then this is problematic.[62] Such «take it or leave it»-designs are a major challenge.

The requirement that consent must be explicit means that it must be clear and unambiguous. There are no particular requirements regarding form. In order to constitute an explicit consent, an active action from the individual is normally required. In a digital world, it will be possible to offer many different designs allowing the user to give consent. The key point here is that any given design must allow the user to actively signal that he or she gives consents. For example, it is not sufficient to provide information about the processing of personal data which takes place on a website along with a sentence which states that you consent when using the service.

The requirement that consent must be informed entails that the person concerned must be sufficiently informed to understand what he or she is consenting to. The individual must subsequently be informed about the nature of the data that is being collected, what the information will be used for, who is responsible and all other information which is required for the data subject to understand what he or she is allowing by way of consent. It may typically be necessary to provide information about when the information is deleted, whether it is shared with others, and to whom it may be shared. The information must be presented in a simple and comprehensible manner.

Consent must be given before processing begins. It must also be possible to withdraw consent, in which case the legal basis for processing ceases to exist. There must be a mechanism for consent to be withdrawn.

Setting up a mechanism which allows the data subject to object to processing (an «opt out»-design) does not mean that consent is achieved if the person does not opt out. Not objecting is not the same as consenting.

The Article 29 Working Party has stated in several opinions that processing personal data in relation to behaviour-based marketing on the Internet requires consent according to these principles.[63]

Other important obligations

The legal basis requirement is just one of several basic obligations. The Norwegian Personal Data Act includes several obligations that must be fulfilled in any processing of personal data.[64] All the obligations have independent significance and represent independent barriers. We will take a closer look at some of the obligations.

---

[60] Example taken from Borgesius, op. cit.

[61] See section 2 no. 7 of the act.

[62] The Article 29 Working Party has for example in working document 02/2013 pages 5 and 6 stated that it is fundamental that Internet-based services cannot be conditional on the user accepting cookies. – there must be a genuine choice.

[63] See opinion 2/2010, 16/2011 and working document 02/2013

[64] Cf. section 11

The purpose limitation principle

Personal data must only be processed for expressly stated and legitimate purposes. [65] The controller has to clarify what the purpose is – both for itself and for the data subject This purpose must be clear when processing begins, in other words when the information is collected or registered. The purpose sets out a clear framework describing what the information can and cannot be used for.

In order to emphasize the significance of sticking to the original purpose, the act prohibits processing the information for new purposes, that is purposes incompatible with the original one.[66] The only exception from this prohibition is if the data subject consents to processing for the new purpose. A new purpose will typically be incompatible if it differs significantly from the original purpose and/or exceeds what the data subject could reasonably expect. For example, registering the behaviour of the users of a website in order to develop and operate the website effectively would be something markedly different from creating personal profiles of individual users for individually customised marketing.

The purpose limitation principle is doubly significant in relation to the use of personal data for marketing. First of all, it restricts the ability to make use of information which was originally gathered for purposes other than marketing. Secondly, it limits the opportunity to make use of information gathered for marketing purposes for alternative and new purposes.

In practice, it represents a challenge when information collected for the purpose of marketing is used for other purposes. For example, Microsoft states in its privacy statement: «Because the data used for interest-based advertising is also used for other necessary purposes (including providing our services, analytics and fraud detection), opting out of interest-based advertising does not stop that data from being collected.»[67]

Limitations of scope and time

According to the Norwegian Personal Data Act, the organisation responsible for processing must restrict their processing of personal data to what is relevant and sufficient for the stated purpose, and the information must be deleted when retention is no longer necessary for that purpose.[68] In addition, the information must be accurate and updated.

It follows that controller have to content itself with what is relevant for the purpose and restrict itself to what is sufficient. This limits the scope of the information that can be processed. Excessive data collecting is not legal.[69]

There is also a time limit. It is not legal to keep storing information when it is no longer required for the purpose. The processing of the information must have an end date.

In practice these limitations may overlap. For example, the information may lose its relevance over time and therefore become unnecessary for the stated purpose. In the case of behavioural marketing, information about a user's behaviour from some time previously may be be regarded as outdated, less relevant and unnecessary, and processing of information for this purpose should cease.

Right to information

The personal data regulations are based on a fundamental principle that the processing of personal data must be transparent. There are therefore specific rules about information.[70]

Individuals have the right to be informed when data about them are being processed. The controller must see to this without being prompted. Information about what type of data are processed must always be provided. Similarly, the company must inform the individual about the purpose, who is responsible for the processing and with whom the information may be shared.

In addition there is a specific requirement to advise when someone, for example as part of marketing activities, approaches an individual on the basis of a personal profile which is intended to describe behaviour, preferences, abilities or needs. In such instances information about the controller must be provided, as well as on what types of data are used and

---

[65] For a more detailed review see opinion 03/2013 on purpose limitation

[66] Cf. section 11 letter c.

[67] http://www.microsoft.com/nb-no/privacystatement/default.aspx

[68] Cf. section 11 letters d and e

[69] See the corresponding provision in article 6 c) of the privacy directive, which requires that processing must be «adequate, relevant and not excessive».

[70] Cf. chapter 3 of the act.

where they are collected from. It must be assumed that this requirement applies to the individually customised marketing that takes place via the Internet. Here the act is intended to ensure extra transparency in a situation where the individual may not intuitively understand what is happening.

The individual also has the right to receive, on request, further information about the processing of personal data concerning him-or herself. This includes a right of access to data that is being processed. With regards to behavioural marketing, allowing people access to their own profile may be of particular significance.[71]

Correction and erasure

The Norwegian Personal Data Act gives the individual the right to have information corrected and deleted, subject to additional conditions.[72] Correction in particular may be relevant when information is inaccurate or incomplete. This may for example be significant with regard to personal profiles. A profile may portray the person concerned inaccurately and it must be possible for the individual to have the impression of him- or herself corrected.

Erasure may be relevant when the individual objects to processing, for example by withdrawing their consent, when there is no legal basis for further processing. Erasure may also be relevant when the processing does not comply with the basic requirements – for example because the information is outdated and irrelevant to the purpose, or because further processing is unnecessary for the stated purpose.

The Norwegian Electronic Communications Act

Section 2-7 b of the Norwegian Electronic Communications Act states a specific rule about the use of cookies.[73]

The provision is often called *the cookie provision*, and it has also been given the heading «Use of cookies». This is somewhat misleading as the provision covers every situation in which someone stores or gains access to data in the user's device. The provision may for example also apply to so-called device fingerprinting[74] or to the installation of apps or other software.[75] The rule in the act is based on the understanding that users' devices are part of an individual's private sphere, and that storing data on them or retrieving data from them represents a form of intrusion. This applies independently of the fact that information which is stored or retrieved is to be regarded as personal data.

The act implements article 5 (3) of the EU's ePrivacy directive[76]. The provision is directed at a specific act – storing or gaining access to information in the user's device, for example placing a cookie in the user's web

The «Cookie Provision»

«Storing information in the user's device, or gaining access to this, is not permitted unless the user is kept informed about which information is processed, the purpose of this processing and who will process the information, and consents to this.

The first point is not an obstacle to technical storage or access to information

1. exclusively for the purpose of relaying communication in an electronic communications network
2. which is necessary to supply an information-based societal service in accordance with the user's explicit request. »

Section 2-7 b of the Norwegian Electronic Communications Act

71 Companies such as Google and Microsoft have begun to make arrangements for this.

72 Cf. sections 27 and 28.

73 Cf. section 2-7 b.

74 Technical information about the device is gathered and used to make the device uniquely recognisable. See the Article 29 Working Party's opinion 09/2014 on the application of the Directive 2002/58/EC to device fingerprinting.

75 See the Article 29 Working Party's opinion 02/2013 on apps on smart devices.

76 The ePrivacy directive (Direktiv 2002/58/EF).

browser. This is prohibited unless the user is given sufficient information and has consented[77].

It follows from the preparatory work for the Norwegian Electronic Communications Act[78] that the consent requirement is not the same as the consent requirement contained in the Norwegian Personal Data Act. The ministry points out that there are practical considerations behind this: «A technical setting in a web browser could be used to give consent or refuse consent, provided that the end user is sufficiently informed about the purpose of saving and storing information. A default setting in a web browser that the user accepts cookies is also regarded as representing consent.» In other words, the preparatory work paves the way for it to be sufficient to provide clear information about the use of cookies. As long as the user has not adjusted the setting in their web browser to reject cookies, there is no obstacle to placing them on the user's device.

The ministry provides further grounds for its view:

«The ministry considers it fundamental that article 5.3 of the ePrivacy directive is not intended to make the use of legally permitted techniques such as cookies more difficult, but to ensure the privacy of users. Article 5.3 is primarily directed at techniques that violate privacy, such as spyware and the like. The ministry therefore wishes to emphasise that the change in the regulations is not intended to involve any change when it applies to using legally permitted techniques, but that the change must be understood as precisely defining the obligation to give users sufficient information and options with regard to the use of these techniques. This will give users the opportunity to safeguard their rights. 'Legally permitted techniques' means cookies or similar techniques which are widespread, and which are normally used as purely technical aids in setting up websites.»

We believe consent under the Norwegian Electronic Communications Act section 2-7 b must be compatible with the Norwegian Personal Data Act's requirements for consent.

The obligation under the directive is a clear change from previous regulations[79]. The previous provision in article 5 (3) of the directive required that the user should have cause to object. This was changed so that consent must be obtained from the user instead.

It follows from article 2 (d) of the directive that the term 'consent' must correspond to consent in the sense of the Data Protection Directive - that is, the directive which the Norwegian Personal Data Act implements.

Furthermore, the ministry's reference to cookies as a legitimate technique is difficult to understand. The purpose of the cookie and how it is used determines its legitimacy. For most legitimate types of cookies, the kind that are necessary for a service to function, there are explicit exceptions from the consent requirement. For other types of cookies, the purpose of which is for example gathering information for behaviour-based marketing, and that are used to follow the individual across services, the position is different. Here consent is required. It is not until consent is given that using cookies as a technique for data collection is legitimate. It is therefore not tenable to say that cookies are a legitimate technique per se and to use this as an argument for it being sufficient that the user has not objected to cookies in their web browser's settings.

Finally, there are grounds for highlighting that the Article 29 Working Party has repeatedly rejected the view that settings in the web browser or other opt-out mechanisms are compatible with the consent requirement according to article 5.3 of the ePrivacy directive. The consent requirement must be compatible with consent in the sense of the Data Protection Directive, according to the Working Party.[80]

If the Norwegian Electronic Communications Act's consent requirements in section 2-7 b must be interpreted according to the statements in the preparatory work, there is a risk of conflict between the Norwegian regulation and the directive which the regulation is intended to implement. It is assumed that Norwegian law complies with our obligations under international law (the presumption principle), and it may be asked whether the Norwegian Electronic Communications Act should be interpreted and applied in such a way that conflict does not arise.[81]

---

[77] We do not address the exception in the second point in further detail here.
[78] Prop. 69 L (2012-2013) page 43.
[79] In directive 2009/136/EC.
[80] See the opinions mentioned in footnote 67 above.
[81] See Rt. 2000 page 1811 (Finnanger I).

Who undertakes to comply with «the cookie provision»?

As has been stated, section 2-7 b of the Norwegian Electronic Communications Act regulates a specific action - storing or obtaining access to information on the user's device. It is the legal person who is behind the action – and who determines its purpose and the methods used – who is responsible for complying with the act82. The legal person responsible according to the Norwegian Electronic Communications Act is not necessarily the controller in the sense of the Norwegian Personal Data Act. This is due to the fact that information which is stored or retrieved is not necessarily regarded as personal data.

When a user visits a website, for example a newspaper, the person concerned will often come into contact with several players who use cookies or other techniques to store or obtain access to information about the user's device. This will typically be the media company which runs the website, and other players (often called third parties) who for example carry out marketing or analysis activities.

In such a situation, every player will in principle be responsible for informing users and obtaining consent where this is required. The Norwegian Communications Authority considers it fundamental that the legal person who permits the use of third-party cookies on their own website must provide information about this in addition to information about its own cookies. [83] At the same time the Norwegian Communications Authority states that the third party is responsible for fulfilling the informing obligation on its own website.[84]

The Norwegian Data Protection Authority believes that the user should be given the required information on the website he or she is visiting. Both the owner of the website (the publisher) and the various third parties are responsible for providing information and obtaining consent, and here the players should collaborate so that the information is provided in one place. Publishers should make arrangements for third parties to provide information about their cookies and other actions covered by the provision directly on the publisher's website.

Territorial scope of the «cookie provision»

Section 2-7 b of the Norwegian Electronic Communications Act is intended to protect the person using an electronic device. Exactly how far does this protection go? Do foreign companies/players have to comply with Norwegian law when they use cookies or similar on Norwegian users' devices?

This problem is not discussed nor directly resolved in the preparatory work. Based on the general provisions regarding the scope of the law in sections 1-2 and 1-3 of the Norwegian Electronic Communications Act, the act appears to apply to the legal person conducting activities linked to electronic communications on Norwegian territory[85].

The Article 29 Working Party has stated on several occasions that it is fundamental that article 5 (3) of the ePrivacy directive is directed at everyone who stores or gains access to data on a user's device, regardless where in the world the responsible person concerned may be. [86] The Article 29 Working Party points out that article 5 (3) distinguishes itself from many of the other provisions in the directive, which is mainly directed at providers of electronic communications networks or services in the EU: It shall protect the individual against a specific type of action, regardless of who is behind the action or where in the world this person may be. The Article 29 Working Party also believes that the ePrivacy directive must be interpreted in the light of the Data Protection Directive's provision regarding territorial extent (article 4). This directive – or more precisely the act in the country implementing the directive – will apply to players who are not established in an EU country but use equipment in the EU country when processing personal data. As stated previously, the term'equipment' could cover electronic devices when the company responsible for processing uses these devices as part of its processing of personal data, for example by placing a cookie which records personal data.

Unfortunately, the extent of the territorial scope of the Norwegian act is uncertain. It is however reasonable to

82 See the preparatory work Prop. 69 L (2012-2013) page 102

83 The Norwegian Communications Authority is the supervisory authority according to the Norwegian Electronic Communications Act.

84 http://www.nkom.no/teknisk/internett/cookies/information capsules-cookies

85 Section 1-3 of the Norwegian Electronic Communications Act expands the territorial scope so it applies to Norwegian ships and planes.

86 See opinion 01/2008, 02/2010 and 03/2013

expect that foreign players who target their activities at the Norwegian market, for example by offering marketing services, must comply with Norwegian law in dealings with Norwegian users.

The relationship between the acts

Section 2-7 b of the Norwegian Electronic Communications Act and the Norwegian Personal Data Act apply side by side. Section 2-7 b of the Norwegian Electronic Communications Act only regulates the action of saving or gaining access to information on the user's device, completely independently of whether or not the information is personal data. If personal data are processed the provisions of the Norwegian Personal Data Act also apply in full. This means that the person who gathers personal data through actions covered by section 2-7 b of the Norwegian Electronic Communications must act in accordance with both sets of rules.

However, a salient point is whether section 2-7 b of the Norwegian Electronic Communications Act is an independent legal basis for the processing of personal data (lex specialis), or if on the other hand, the processing of personal data must have a legal basis according to the standard provisions of the Norwegian Personal Data Act. As stated, the consent requirement in the Norwegian Electronic Communications Act as it appears in the preparatory work, does not satisfy the corresponding requirement according to the Norwegian Personal Data Act. Will consent according to the Norwegian Electronic Communications Act provide the required legal basis for processing personal data?

According to section 8 and section 9 of the Norwegian Personal Data Act a specific processing of personal data is permitted if it is stipulated in law that there is access to such processing. Here "law" means an act other than the Norwegian Personal Data Act.[87]

Is section 2-7 b of the Norwegian Electronic Communications Act a special provision about a type of processing of personal data?

The Norwegian Data Protection Authority is likely to take the view that section 2-7 b of the Norwegian Electronic Communications Act is *not* a specific rule about the processing of personal data – it does not regulate the processing of personal data as such. Even though the underlying motive for the rule is privacy protection, the provision does not by nature involve the protection of personal data. On the contrary, the rule is based on the individual's device being part of the private sphere of the person concerned. It will provide protection against intrusions into this sphere by actions such as those described by the rule – completely independently of what kind of information is stored or retrieved. If storing or gaining information on the equipment also means that personal data is processed then the protection of personal data comes into play[88].

Neither the wording of the provision nor the preparatory work state anything specific about the provision specifically regulating a particular type of processing of personal data. The relationship to the Norwegian Personal Data Act is not affected, apart from it being stated that the consent requirement differs from that which applies according to the Norwegian Personal Data Act.

The Norwegian Data Protection Authority therefore believes that the consent requirement according to the Norwegian Personal Data Act would prevail in situations in which personal data are processed. If this is the case, it means that the legal person collecting and processing personal data with the help of actions covered by section 2-7 b of the Norwegian Electronic Communications Act must actually have consent which is compatible with the consent requirement in the Norwegian Personal Data Act. It is not sufficient just to act according to the consent requirement in the Norwegian Electronic Communications Act.

A new legal framework

In the EU, work is now being done on a new legal framework that will replace the current Data Protection Directive. It is expected that the EU will reach its goal for a new regulation in the near future. The regulation will probably be incorporated straight into Norwegian law. In its current form the proposal is based on the

[87] The Norwegian Personal Data Act is in itself an act which stipulates that it is legal to process personal data

[88] There is a corresponding argument in legal theory, see Zuiderveen Borgesius op. cit. The Article 29 Working Party can however be understood as meaning that article 5 (3) of the ePrivacy directive, which the Norwegian Electronic Communications Act implements, is lex specialis in relation to the Data Protection Directive when it comes to the legal basis requirement. But as stated, the group is of the opinion that the consent requirements in the two sets of rules must be compatible, so that someone who is granted consent under article 5 (3) is simultaneously granted consent in the sense of the privacy directive for any processing of personal data which are gathered.

existing directive, but in all probability there will be significant changes. [89] We will mention some:

In principle, the proposal is based on known material regarding **the territorial scope**. The regulation will apply when the controllers established in the EU, and when the processing takes place in context of activities of that etablishment. There is, however, one important change. The proposal includes data processors in such a way that the regulations will also apply when only the data processor[90] is established in the EU. This is a clear expansion.

In instances where the establishment criteria have not been fulfilled, changes are proposed which clearly show a desire to expand the scope of the regulation. The proposed legal framework will apply when personal data is processed about individuals who are residents in the EU, provided that the processing is related to the offering of goods or services to these individuals in the EU, or to the monitoring of their behaviour.

In light of this we must assume that the rules will have considerable territorial scope when it comes to the individually customised marketing which takes place on the Internet.

As a point of departure it is proposed that the principle of **purpose limitation** is continued in the future regulation.

At the same time there is a proposal that personal data can be processed for new and incompatible purposes, provided that the processing has a legal basis in the regulations. This means that consent is not necessarily required for using the information for completely different purposes.

The proposal has justifiably encountered great resistance here. In its draft form, Parliament has not restricted the purpose limitation principle, so here it is very unclear what the final result will be.

If the Commission or the Council's proposals become applicable law, there is reason to fear that predictability (only processing information for stated purposes) will become significantly worse.

It is proposed that the principles of **consent** continue – it must be freely given, informed and specifically stated.

Several rules have also been proposed which precisely define the meaning of consent. It is proposed that the burden of proof that consent has been given lies with the organisation responsible for processing. This will make the requirement that it must be possible to document the data subject's acceptance of processing more stringent.

It is also proposed that if consent is to be given in context of a written declaration which also deals with another matter, the requirement to give consent must be presented distinguishable in its appearance from this other matter. This could affect the use of user agreements (terms and agreement) which include how personal data are processed. This is an important clarification that consent to process personal data is something different to entering into a general agreement, and that they should be kept separate.

Parliament has also proposed that the execution of a contract or a service cannot be conditional on consent being given to process personal data if the personal data are not required to execute the contract or provide the service. Such a rule will strengthen the voluntary element of consent to a great degree. In practice, the fact that the individual does not have a genuine opportunity to say "no" if they want to make use of an Internet service is an extremely challenging issue.

Specific rules for **profiling** which will enhance the individual's right not to be profiled have been proposed. The rules are specifically aimed at measures based on automated processes, including profiling, and where the measure has legal significance for the individual or which clearly affect the person in some other way.

The rules must be assumed to have significance for custom marketing in a digital, networked world.

The significance of consent is increased in the proposal, and limitations are placed on access to processing sensitive information as part of the profiling.

[89] The Commission, Council and Parliament have all produced proposed legal texts. The wording of these differs somewhat. Negotiations are now taking place to achieve uniformity.

[90] A data processor is someone who processes personal data on behalf of the person or the organisation responsible for processing.

Privacy challenges

The advertising income from behavioural marketing contributes to financing a huge amount of free Internet services. We can enjoy access to newspapers, translation services, e-mail, music and videos without paying for it. But personalised and targeted advertising also challenges privacy.

From a privacy perspective, the greatest challenge is that enormous amounts of personal data about us are collected out of sight. The ordinary Internet user does not have any awareness of which data are collected about him or her, how this is done, who processes the information, the scope of how they are used and what consequences the use of the data has for them. If we are to ensure a good level of privacy this requires openness, transparency and accountability. The current global advertising market is closed, complex and opaque.

Information asymmetry

Very few Internet users realise that dozens of companies are present behind the scenes collecting personal data when they surf the web. We now have a society that resembles a one-way mirror in which thousands of companies know a great deal about us while we hardly know anything about them.

«Once people realise what's happening, I can't imagine there won't be pushback.» [91]

The right to information is central to privacy. This is regulated by the European Data Protection Directive, for example through the right to be informed. Without information and knowledge about what is going on, we are not in a position to be conscious and critical consumers.

The market is characterised by information asymmetry. Since the 1970s, economists have been preoccupied by this phenomenon and have studied how insufficient information results in the consumer being unable to assess *the quality* of the product or service he or she is buying.[92] One consequence of the consumer being unable to recognise quality is that vendors will not compete on quality. Information asymmetry may lead to consumers being offered products and services of steadily decreasing quality: a race to the bottom. Information asymmetry is therefore described as a form of *market failure* and from an economic perspective it justifies regulatory intervention by the authorities. [93]

When visiting a website, it is almost impossible to know how much information is being collected about us and how this information is used. The consumers' knowledge deficits means that companies are not given the necessary incentives to compete in their efforts to provide the consumer with privacy-friendly services. Consumers are not in a position to recognise quality, here meaning services that do not allow third parties to collect personal data behind the scenes, and are therefore not willing to pay for it. If people do not know that their data is collected they cannot demand or value services which allow them to be left alone. The uneven distribution of information results in a competitive situation that encourages the market players to use methods that to an increasing extent are invasive of people's privacy.[94]

In such a situation, competition in the market will not balance the accounts. Services and products which are based on the users being left alone and which may represent a genuine alternative for most people do not emerge.

91 Quote from the head of a British media agency, cited in The Economist, "Little Brother, Special Report on Advertising and Technology", 13.09.2014, http://www.ogilvydo.com/wp-content/uploads/2014/09/20140913_SR_MAILOUT.pdf

92 Sørgard, Lars, «Informasjonsasymmetri og konkurransepolitikk» [«Information asymmetry and competition policy»], published in: Stortingsmelding [Norwegian parliamentary report] no. 15 (2004-2005): Om konkurransepolitikken [About competition policy], Appendix 1, p 95-109, Department of Economics, The Norwegian School of Economics, Bergen, 2005

93 Zuiderveen Borgesius, Frederik J., «Behavioural Sciences and the Regulation of Privacy on the Internet», draft chapter of the book, «Nudging and the Law - What can EU Law learn from Behavioural Sciences?», ed. A-L Sibony & A. Alemanno (Hart Publishing), Institute for Information Law Research Paper No. 2014-02, Amsterdam Law School Research Paper No. 2014-54, 2014, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2513771

94 Ibid.

Weaknesses of consent

When designing services where use is based on consent to a set of terms, it follows that for the consent to be valid, the user must be presented with a clear choice between yes and no. There is however reason to ask whether the individual can make a choices between genuine alternatives.[95]

It is very difficult for most people to familiarize themselves with what is happening behind the scene online. In practice, the individual has little opportunity to make informed decisions. This is partly linked to the lack of transparency, and partly to the fact that the information provided by the different agents is difficult to comprehend for most people.

A survey conducted in the USA shows that people state 'resignation' as the main reason for giving out their personal data in exchange for free services.[96]

The survey indicate that marketers are misrepresenting a large majority of Americans by claiming that Americans give out information about themselves as a trade off for benefits they receive. To the contrary, the survey reveals most Americans do not believe that 'data for discounts' is a square deal. The findings also suggest that Americans' willingness to provide personal information to marketers cannot be explained by the their poor knowledge of the ins and outs of digital commerce. In fact, people who know more about ways marketers can use their personal information are more likely rather than less to accept discounts in exchange for data when presented with a real-life scenario. Rather than feeling able to make choices, Americans believe it is futile to manage what companies can learn about them. The study reveals that more than half do not want to lose control over their information but also believe this loss of control has already happened.

The challenges related to consent are also linked to human behaviour. We are often less rational than we like to think. We also have a tendency to choose the option that maintains the status quo, options or the one which offers an immediate and positive return. If, for example, a customer visits an onlineshop to buy a product then the act of buying the product will be the primary focus for the customer. Having to find out how personal data are processed represents a time cost to the customer in addition to everything else the customer is presented with, such as the standard terms and conditions of sale. The customer will usually be concerned about the short term purpose of the visit, i.e. buying the product, and will almost automatically accept everything they are asked to accept. Opt-out designs are rarely used because we tend to use the default choice that is offered.

Such human qualities — or weaknesses, if you prefer — can be exploited. This is presumably also the case.

It follows from this that to be realistic, we should admit that making the processing of personal data subject to consent often does not have the intended effect. By letting individuals decide for themselves, the individual is also left to stand alone against big and powerful agents who in reality can dictate the terms he or she must consent to.

Risk of manipulation

The imbalance of power between those who profile and those being profiled is becoming greater. This challenges our personal autonomy, because the great information asymmetry increases the risk of manipulation.[97]

We used to make purchases face-to-face in a shop. Today's consumer purchases products or services through some interactive or networked device, computer, smart phone or tablet. Today's consumer has become a «mediated« consumer.[98] This has various consequences. First of all, the services and products we deal with collect and store enormous volumes of data about us. Secondly, companies can increasingly choose

95 For a more broad-based review see Zuiderveen Borgesius, Frederik J., «Behavioural Sciences and the Regulation of Privacy on the Internet», op. cit

96 Turow, Joseph, Michael Hennessy and Nora Draper, «The Tradeoff Fallacy, How Marketers Are Misrepresenting American Consumers And Opening Them Up to Exploitation», Annenberg School for Communication, University of Pennsylvania, 2015,

97 The Council of Europe believes that the increasing use of profiling represents a threat to the individual's opportunity for self-determination, see the Council of Europe, «Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling», 2010, https://wcd.coe.int/ViewDoc.jsp?id=1710949

98 Calo, Ryan, «Digital Market Manipulation», 82 George Washington Law Review 995 (2014); University of Washington School of Law Research Paper No. 2013-27, 2013, http://dx.doi.org/10.2139/ssrn.2309703

when they want to approach consumers, rather than wait until the consumer has decided to enter a market context. The fact that companies may contact the consumer rather than vice versa is affecting the relationship between seller and buyer. We do not have the opportunity to assume the role of critical consumer before we enter a purchasing situation in the same way. In an age of constant screen time we are constantly in a purchasing situation. These two things, companies' enormous knowledge combined with their constant access to us, make us vulnerable to manipulation

In today's market, advertisers are concerned about relevance. Advertisers show users adverts for products they believe they want, based on the digital footprints left by users. However, the trend is towards data also being used for analysis aimed at identifying people's *vulnerabilities* and personality traits. The advert must not only be relevant with regard to the user's interests, it must also be in a form that is adapted to the individual's personality. This type of profiling is called *persuasive profiling*. Data analysis can, for example, reveal whether people are impulsive or cautious, whether they respond well to visual messages or advertising with a lot of text, whether they like being the first to have the latest innovation or whether they react best if they hear that a product is almost sold out.

In future, personalised marketing may become so effective that the advertisers gain an unfair upper hand over the consumers. This will challenge the individual's autonomy and right to self-determination. Companies who collect data about us know us so well that they can push us in precisely the direction they want. Because we do not have sufficient knowledge about how the advertising market works, this will happen without us being aware of it.

Risk of wrong decisions

It is a fundamental requirement of the Norwegian Personal Data Act that companies who process personal data must ensure that the information that is processed is accurate. The profiles used for behavioural advertising often consist of data the companies have gathered themselves, combined with data gathered from external sources. It is particularly the quality of the latter, so-called third-party data, which may be of variable quality. For example, cookie data does not provide factual information about an individual, but the analysis of cookie data provides the basis for making assumptions about an individual's gender, age, place of residence, interests, habits and so on. Data collected from social media do not produce verifiable information about individuals, either. There is a real risk that incorrect information will be assigned to identified or identifiable individuals when this type of data is used in building user profiles. When incorrect decisions are made because someone is assessed on the basis of inaccurate data, this represents a threat to the individual's right to fair treatment.

In this context the right to be informed about which data is collected and how it is processed is key. The right to be informed entails that the individual can demand that inaccurate information, assessments and claims are corrected or deleted. However, the consumer has very little leverage here, simply because it is almost impossible to discover the extent to which data-collectors have made the wrong inferences about you. If you do discover that incorrect inferences have been made, it is difficult to know which company to contact. The company in question is more likely than not to be based in another country than you and does in all likelihood not share data with foreign citizens. Also, it may not be under the jurisdiction of European law, which confers the right to be informed.

Hidden discrimination

Profiling increases the risk of unjustified and hidden discrimination. Even in cases where the data forming the basis of the decision are accurate, they may produce an unfair and discriminatory result for the individual. There is a growing burden of proof that automated marketing controlled by algorithms may cement existing prejudices and stereotypes. There is a widespread view that software and algorithms dependent on data are objective. But algorithms do not have a value-free existence, devoid of human influence. The algorithm is written and maintained by people, and adjust on the basis of behavioural data. As a result algorithms can reinforce human prejudices. [99]

Google's Internet-based advertising system, for example, displayed an advert for high-income jobs to men more often than it displayed the advert to women, and researchers have discovered instances where advertising for credit loans was shown only to people in low-income districts.[100] It has also been discovered that

[99] The New York Times, «When Algorithms Discriminate», 9.7.2015,

[100] Ibid.

profiling can result in price discrimination. The Wall Street Journal found that a web shop changed its prices according to where the user was.[101]

It is very difficult for consumers to detect this type of discrimination. The ordinary consumer has little insight into this market and cannot look into whether algorithms are constructed in ways that lead to discrimination. Not even the companies who have developed the algorithms are necessarily aware that they have a discriminatory effect. It is therefore of great importance that companies revise their algorithms regularly to prevent them from having such an outcome.

The risk of using data in ways which have discriminatory results for individuals was one of the reasons why a demand was made to the credit-reference industry to become more open and transparent. As the consequences of having a poor credit rating are so consequential, the sector has had strict requirements imposed to do with transparency and openness. Credit reference agencies operate under licences granted by the Norwegian Data Protection Authority, which specify which data can be used in assessments when companies have to make decisions about people's creditworthiness.

Wide-ranging purposes

A milestone with regards to the collection and utilisation of personal data about was reached on 1 February 2012. On that date Google implemented extensive changes to its privacy policy. Google branded this a *simplification* of the policy. The simplification consisted of introducing one common privacy policy for all Google's services. The simplification meant that information collected from one service, for example YouTube, could be utilised across all the company's services, for example to advertisers in order to sell targeted advertising.[102] Not long after Google implemented this crucial change, other major Internet players followed suit. Facebook, Microsoft and Yahoo made corresponding changes to their privacy policies in the course of 2012.

It is a fundamental privacy principle that personal data can only be collected and used for clearly defined purposes. [103] The opportunity which Big Data analysis offers for comparing and analysing data from many sources represents a challenge to the principle of purpose limitation. In order to be at greater liberty to share and utilise data across services, there is now a trend of almost all major Internet players using the same broad justification of purpose, of this type:

> *«The information is collected in order to develop the service and improve your user experience».*

Such a purpose gives the companies an extre**m**ely free hand to utilise the information they collect from users. This is unfortunate from a privacy perspective, because the individual then loses control over how their information is used.

If people feel that they are losing control over their own personal data and do not know for what purpose the information may be used, this may result in people beginning to constrain themselves. It may for example result in people avoiding reading certain articles in a newspaper, because they are uncertain what consequences the analysis of their reading habits may have. We refer to this phenomenon as «the chilling effect», and is a direct consequence of addressing privacy poorly.

Aggressive mapping

Many people feel uncomfortable about being mapped in detail.[104] The right to privacy means that we must be able to have a few different spheres in our private lives that are respected by all companies who collect and process data. Building profiles involves mixing

[101] The Wall Street Journal, «Websites Vary Prices, Deals Based on Users' Information», 21.12.2012,

[102] In October 2012 the European privacy authorities sent Google a letter containing the requirement that the company should implement a number of changes in order to comply with the European privacy directive, 95/46/EC: http://www.cnil.fr/fileadmin/documents/en/20121016-letter_google-article_29-FINAL.pdf

[103] Cf. the Norwegian Personal Data Act section 11 first paragraph letter c)

[104] The Norwegian Data Protection Authority regularly receives messages from members of the public reacting to the way marketers gather information and stating that they do not feel they have control over how the information is used.

information from many different spheres of someone's life. Such sharing of data across areas of life may create a feeling of being monitored.[105]

By introducing log-in solutions in which the users are continuously logged in, companies can accumulate enough information to create very detailed profiles which over time can produce a complete and accurate picture of someone's private identity. The data protection authorities in Europe will most likely be confronted with advertisers and publishers wishing to store customer data for a long time in order not to lose out in competition with companies based in the USA. By tracking users over a period of years, publishers and marketers can see how consumption patterns change through the various stages of life. They will be able to see when various life events occur, for example a user moving away from home, getting married or having children. We have seen that there is a great willingness to pay for such data in the marketplace.

«Google's privacy policy is to get right up to the creepy line and not cross it.»

Erick Schmidt, Executive Chairman & former CEO, Google[106]

The longer data are stored, the larger the multitude of facets of a person's life and identity will be mapped. Storing data for a long time in order to build up comprehensive profiles of individual users may therefore come into conflict with the principle of proportionality, which means that it will come to represent an intrusion into the individual's right to privacy that is deemed unacceptable.

Big Data analysis may also reveal information that the individual has *not* consented to sharing. New personal information, information that may be sensitive, may be inferred from the analysis of personal data. For example, this was the case in the much-used Target example: An American retail chain had an algorithm developed that revealed whether customers were pregnant based on which products they bought. When collecting and analysing some types of data, for example location data and sensor data from wearables, the risk of revealing sensitive information about the user is particularly high.

The major Internet companies and the advertisers are careful not to utilise the information they gather in such a way that the user finds it intrusive or unpleasant. Nevertheless, the players will constantly try to collect as much information and target advertising as much as possible without crossing the line into what the individual consumer regards as being «creepy». If deemed to intrusive by consumers, the companies bide their time. Consumers will soften up and their perception will change after a while.

In 2011 the Norwegian Data Protection Authority wrote about how Facebook has continuously changed its privacy policy and conditions since its start up in 2008.[107] By taking one step at a time, new policy is incorporated without the customers leaving the platform. An example of this was Facebook's attempt to introduce face recognition. This feature was strongly criticised by authorities and consumers in Europe, with the result that its implementation was brought to a halt. In other parts of the world where protests were fewer, the feature was implemented.

Further, storing enormous amounts of data about individuals represents a risk in itself. The consequences of data security breaches and data leaks are even greater if large and comprehensive datasets that provide a rich and revealing picture of individuals end up in the wrong hands.

Danger of re-identification

Marketers claim that they do not use identifying information when they build profiles. Rather, profiles consist of aggregated and anonymised information that cannot be linked back to a unique individual, they say. Nevertheless, as an anonymous user profile gradually comes to contain more data, it will gradually become very descriptive. Profile xyx is that of a man, 44 years old, divorced, resident in Norwegian post code area 0655, owner of a bird dog, interested in hunting,

105 Polakiewicz, Jörg, «Profiling – the Council of Europe's Contribution» in the collection of articles «European Data Protection: Coming of Age», Ed: Gutwirth, Serge, Ronald Leenes, Paul de Hert and Yves Poullet, Springer, Dardrecht, 2013

106 Business Insider, Eric Schmidt: Google's Policy Is To «Get Right Up To The Creepy Line And Not Cross It», 01.10.2010, http://www.businessinsider.com/eric-schmidt-googles-policy-is-to-get-right-up-to-the-creepy-line-and-not-cross-it-2010-10

107 The Norwegian Data Protection Authority, «Social Network Services and Privacy A case study of Facebook", 2011, http://www.datatilsynet.no/Global/english/11_00643_5_PartI_Rapport_Facebook_2011.pdf

probably looking for a new car. This is probably a description that does not fit more than a handful of people, perhaps just one person. The more data are included in a profile, the more challenging it is to safeguard the anonymity of the person who is profiled.

By aligning data from several sources, it is possible to identify individuals from what are in principle anonymous data sets. [108] Big Data technology has blurred the boundary between anonymous information and personal data. Studies have shown that knowing the post code and date of birth of an individual is enough to reveal someone's identity. There are also some types of data it is more challenging to render anonymous than others. One example is location data. A group of researchers studied location data that had been made anonymous for one and a half million people, and by aligning just four indications of time and place, they succeeded in identifying 95 per cent of the individuals in the data set.[109]

With an increased risk of re-identification, it becomes important that companies who create profiles perform thorough risk assessments when they anonymize collected data. It is also important that companies engaged in profile building are aware of the difference between pseudonymous data and anonymous data. The former data type is still regarded as personal data, even though directly identifying indicators have been removed from the data set.

Flow of information out of the EU

The majority of the third-party companies present on Norwegian and European websites are based in the United States. This means that large volumes of personal data about European citizens flow out of Europe and are processed under different rules than the European ones. This represents a challenge to the privacy of Europeans. .

According to the so-called Safe Harbor Framework Agreement, the USA should be regarded as a country with adequate protection of personal data when data were transferred to American companies which had signed up to the scheme. In light of the Snowden revelations, questions were asked about whether the Safe Harbor agreement provided adequate security for personal data transferred to the USA. The agreement was ruled to be invalid by the Court of Justice of the European Union in October 2015, and it remains unclear how the issues related to transferring personal data to the USA best can be resolved for the future. [110]

Following pressure from the authorities, data providers in the USA such as Axciom and Experian have created transparency tools that let users see and edit some of the information the companies have about them. These tools are however only available to residents in the USA. Even though Axciom's data silos very probably contain information about European users, it is not possible for European citizens to find out about data pertaining to themselves.

108 Read more about the risk linked to re-identification and the use of Big Data in the Norwegian Data Protection Authority's report «Big Data, Personvernprinsipper under press» [«Big Data, principles of privacy under pressure»], 2013.

109 de Montjoye, Yves-Alexandre, César A. Hidalgo, Michel Verleysen and Vincent D. Blondel, «Unique in the Crowd: The privacy bounds of human mobility», Scientific Reports 3, Article number: 1376, 2013, http://www.nature.com/articles/srep01376.

110 http://curia.europa.eu/juris/document/document.jsf?text=&docid=168421&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=553887.

Recommendations

In an ideal world, in which the individual's right to privacy is respected by everyone:

- We could read an online newspaper and use other Internet-based services without a hoard of unknown companies looking over our shoulder
- It would be simple to choose what information about us is collected and what it could be used for
- Information we enter into one service would not be used by another service for other purposes
- There would be tracking-free alternatives which would be easily accessible for everyone
- It would be simple to find out what our profiles look like.

Summary

In working on this report we have learned one thing in particular: it is difficult to gain an insight into how the market for automated ad trading works . It is almost impossible to obtain a clear picture of what information is collected, how it is collected, how user profiles are built, how long they are stored for and what information is traded between companies. None of the market players takes responsibility for telling us that we are being traded every time we visit a website.

Marketing is by definition about influencing people. Initially we asked how far the advertising industry can go in influencing others before it is no longer acceptable. What methods are acceptable to get someone to act, think or believe in a particular way? As we have demonstrated in the report, it is now technically possible to map an individual down to the smallest detail. Companies can track where we are every hour of the day, register everything we read and search for on the Internet, and based on this create narratives of our lives. Is this acceptable? We believe that the way in which the advertising industry now functions, where mapping largely takes place behind the scenes and is difficult to avoid, is not acceptable.

Privacy is about our right to decide for ourselves what information about us we want to share with others. It is about our right to develop and live our lives without someone constantly monitoring what we do. If we lose control of our personal data, we also lose control of being able to define who we are.

No industry in the world knows more about us than the advertising industry. Nevertheless, we have very little insight into how these companies use the information they collect about us. This affects the balance of power in society. Privacy should not only protect the individual against the constant gaze of authorities, it should also protect us against private companies being able to monitor everything we do. The individual is insignificant compared to a large company. Privacy legislation should remedy some of this imbalance of power by giving the individual rights, so that people can check to ensure that they are not being subjected to unfair or discriminatory treatment. Because the advertising industry is so opaque, individuals have limited opportunity of exercising their fundamental right to privacy in their dealings with it.

The market is characterised by information asymmetry. Information asymmetry is a form of market failure. When consumers have no knowledge or understanding about what is going on, they cannot demand services that provide better privacy. This results in the sector having no incentives to provide services that are more privacy-friendly. The winner in the market is the company who has the most data, and future developments will therefore be characterised by increasingly intensive harvesting of personal data.

The Norwegian Data Protection Authority will work to increase transparency and openness in the Norwegian advertising market. We will also work to create genuine choice for users, plus simple ways of exercising the right to decide.

Because the market does not end at Norway's borders, international cooperation is crucial for developing rules that can be applied in a global context. European data protection authorities must work together to exchange experience, coordinate measures for the sector and attempt to harmonise requirements imposed on relevant players. For example, storage time requirements. The players themselves will press for the longest possible storage times. The privacy authorities must therefore weigh up the companies' interests against the individual's interests.

It is to be hoped that the new privacy regulations will increase the privacy of European citizens. All companies within the EU area must comply with identical

legislation, and this also applies to foreign companies who target European citizens.

Data protection authorities in Europe must also work more closely with consumer and competition authorities to safeguard the interests of individuals.[111] Individuals are not influential enough on their own, and on their own they cannot compel companies to offer more privacy-friendly alternatives. Together with other authorities, we must look at what can be done to ensure that users have more control, better information and access to alternative, tracking-free services.

Recommendations and proposed measures

We have listed our recommendations and the measures we propose. The aim is that in total they will contribute to greater openness and transparency in the advertising market, and give the user more control of his or her own personal information.

Recommendations and proposed measures regarding the collection of data

- **Publishers must take responsibility for all third-party players that visit their sites.** They must provide information on which third-party players are present, why they are there, what information the third parties collect and what the information is used for. This requires greater collaboration between the publisher and the third parties in order to find acceptable solutions for collecting the information in one place. Publishers must ensure that all the players on the site act in accordance with Norwegian and European privacy legislation, and they must be able to give visitors sufficient guarantees that this is the case.

- **Collection of personal data for the purposes of profiling and marketing must be based on active consent**. The individual shall be given the option to say yes or no, easily and voluntarily. All businesses using cookies or other tracking devices to collect information about users must acquire their users' consent in terms of cookie use, and not just leave it to the user to protect him or herself by such action as changing the settings in their browser.

- «**Take-it-or-leave-it» -approaches must be avoided**. Publishers must give all users access to their services, including those who do *not* consent to their information being collected and used for personally customised content and advertising.

  Certain forms of processing of personal data may take place without someone's consent. For example, this may be information that it is essential to process in order for the service to function or in order to honour a contract. In such instances it is reasonable that the person must accept that the information is processed. The person must tolerate this if he or she is to make use of the service.

  If processing is subject to consent *the consent must be based on genuine choice*. The Norwegian Data Protection Authority considers that access to Internet services cannot be conditional on the user consenting to their information being collected and processed for marketing purposes. It is not fair to deal with individuals with an attitude of: «You are not welcome if you do not consent.» Such a practice undermines the essence of consent and respect for the private life of the individual.

  Users of Internet services must be given genuine choices when they are asked if they want to give their consent. They must be able to say «yes» or «no». In this, publishers and other providers of Internet-based services must lead the way, and the data supervision authorities in the EFTA area should apply the consent requirements strictly and intervene when necessary.
  Legislators should presumably also assess relevant measures. In this context, the Norwegian Data Protection Authority is positively disposed towards the European Parliament's proposal that implementing a contract or service cannot be conditional on consent being given.

- **Declarations of consent must be improved.** Such declarations must be clearly and plainly worded. They must be short and easy to understand, and must also include clear information about what data is collected, how it is processed and whether other players have access to

111 European Data Protection Supervisor, «Privacy and competitiveness in the age of Big Data: The interplay between data protection, competition law and consumer protection in the Digital Economy», 2014,.https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2014/14-03-26_competitition_law_big_data_EN.pdf

the information. Declarations of consent must provide information about how the profiles are built up and which data categories the profiles consist of (for example whether the profile consists of information about the user's location, demographic data and data about interests deduced from browsing history). A company collecting personal data must stop using broad purpose formulations of the «we will use your data to improve our services» type. Such formulations do not give the user sufficient understanding about what their information is used for or about the probable future use of the information. The EU's new privacy regulations will probably set stricter requirements than is currently the case for how declarations of consent are drawn up, in order to ensure that users understand what they are consenting to.

- **Provide information in alternative ways**. In order for users of digital services to more easily understand what information those services collect, and what the information is used for, it may for example be useful to use icons. The advertising industry should look at how it can label its pages with icons that tell the user that information is collected for profiling purposes, for example. [112]

- **Marketers must inform the individual** when the person concerned is exposed to individually customised advertising with the help of some form of personal profile. Openness is not just required by legislation, but is fundamentally about respecting the people to whom you wish to gain access to. Respect them by saying why they received this particular advert.

Recommendations regarding use of the information

- **Purpose and relevance must be guiding principles for all processing of data**. Data management platforms have been created with the purpose of linking data from many different sources, first party data and third party data collected from other players in the value chain. Such forms of analysis must not be used in ways that conflict with the European Data Protection Directive, for example on purpose limitation.

- **Data must be deleted.** Storing collected personal data for a long time will lead to companies being able to build up very comprehensive, intimate profiles of individuals. Even if collection of the information fulfils the requirements of specification of purpose and relevance, storing the information for a long time may conflict with the proportionality consideration, i.e. the method may be too intrusive in terms of the individual's right to privacy. Comprehensive databases of personal data also constitute a security risk. The consequences for privacy associated with data security breaches become more serious if unauthorised persons manage to gain access to personal profiles that contain information collected over several years.

- **Illegal to profile using sensitive data.** It is illegal to collect sensitive data and use it for profiling purposes. It should also be illegal to create algorithms that produce information of a sensitive nature, for example an analysis that makes assumptions about whether someone has a weight problem. New privacy regulations are likely to make this illegal.

- **Not permitted to build profiles using cookie-matching**. The Norwegian Data Protection Authority will take a closer look at the practice of cookie-matching in association with the purchase and sale of users on the ad exchanges. The authority will investigate the extent to which companies who bid for users on ad exchanges use the information they receive about users during the bidding process to enrich their own profiles. This should not take place.

- **Regular revision of the algorithms.** It is important that companies who develop algorithms for profiling purposes are aware that the algorithms may produce unintended and discriminatory results. The algorithms and the results they produce must be revised regularly to ensure that the algorithms are functioning as intended.

- **Risk assessments in association with making personal data anonymous.** Anonymisation is an important method for being able to draw valuable conclusions from data

[112] The Article 29 group advocates the use of icons in Opinion 02/2013 On apps on smart devices.

analysis while reducing the risks for the people involved. Anonymous information is not defined as personal data, and processing of such information therefore falls outside the Norwegian Personal Data Act. Anonymizing data is however challenging, and indeed it is more challenging today than it was previously. The enormous volume of publicly accessible data, combined with access to increasingly cheaper and more powerful analytical technology, has contributed to increased danger of re-identification. The distinction between anonymous information and personal data has become less clear. This makes it important to perform thorough risk assessments in relation to anonymizing data, and to use reliable anonymisation techniques.

The Norwegian Data Protection Authority will assess the extent to which sanctions should be imposed on companies who consciously attempt to re-identify information in anonymous data sets they have purchased, or have acquired from another company in some other way. Companies which sell anonymised data sets should include in the contractual conditions a written prohibition on purchasers attempting to re-identify the information.

It is also important that companies who build profiles containing pseudonymous information are aware that pseudonymous information is defined as personal data and therefore must be processed in line with the provisions of the Norwegian Personal Data Act.

Recommendations to promote better ways to inform users and offer them choice

- **Automated informational and disclosure solutions.** Companies should develop automated solutions which give the user access to all the stored data about the person concerned, and the opportunity to have this data disclosed. The information must be disclosed in a user-friendly format.

- **Provide information about the profile.** In order to ensure the greatest possible openness about the building of profiles, the user should be given information about their profile. This means that the individual should be kept informed about how the profile is built up, for example in which segments and categories the user is placed. The individual should also receive information about the sources from which the various personal data are collected.

- **It must be made easier to choose tracking-free alternatives.** The transaction costs associated with opting out of tracking are currently too high. People choose the option that is most easily accessible, and most often this is the option in which you are tracked. The option of saying «no» to tracking should be very visible and easily accessible for the user.

- **Create privacy dashboards.** The user should be given the option of choosing the extent to which he wishes to be tracked in order to receive user-adapted content and advertising. Publishers and other relevant players should develop solutions in which the user himself can select which information can be collected, what the information can be used for, who can have access to the information and so on. Google, Microsoft and Facebook have developed solutions in which the user can control the degree of privacy protection to a certain extent.

Collaboration between the industry and the authorities

- **Good privacy is good consumer protection:** Data protection authorities and consumer authorities should collaborate more closely to ensure greater openness and better freedom of choice for the individual. The targeted marketing which takes place via the Internet raises questions under both the Norwegian Personal Data Act and the Norwegian Marketing Control Act. For example, individually customised marketing is more like direct marketing than generic marketing. Advertisers can now target their marketing at selected individuals on the Internet. As a user of Internet services you do not become the focus of attention by the advertisers as such. You become the focus of attention by individual advertisers who are specifically interested in you. The advertisers can pursue you across different services and ensure that you are exposed to the same marketing again and again. The challenges linked to the collection of personal data on the one hand, and marketing on the other hand, overlap. This applies to such

aspects as issues about an individual's right to decide what he or she may be subjected to.

- **Industry codes of conduct.** Publishers, media agencies and advertisers should get together and produce codes of conduct to contribute to creating greater openness about how the marketplace for targeted marketing functions. Such guidelines should safeguard privacy considerations more adequately than is currently the case. The players in the marketing chain should document compliance with the codes of conduct, and this should be the basis on which the players ask for the consumer's trust.

  The relevant trade organisations should establish ethics committees where the utilisation of personal data for marketing purposes versus consumer privacy considerations is discussed. New business ideas and targeting techniques should be discussed by the ethics committee before being implemented. Trade organisations should also encourage their members to develop new systems according to the principles of built-in privacy. Built-in privacy means that privacy is taken into consideration in all phases of a system's development, in routine operations and in business practices.

- **Developing privacy-friendly targeting systems.** The Norwegian Data Protection Authority will promote research into developing more privacy-friendly targeting systems. There are already researchers who claim to have developed targeting systems which are just as effective as those currently in use, but which safeguard users' privacy by methods which include protecting their identity with the use of anonymisation techniques. [113]

- **Privacy-friendly use of data in marketing on the curriculum**. The ethical use of personal data, and learning about privacy and privacy legislation, should be included in the curricula of universities and colleges that have courses in marketing, journalism and information technology.

[113] Tran, Minh-Dung, Gergely Acs and Claude Castelluccia, «Retargeting Without Tracking», INRIA, 2015, France,

Bibliography

Aftenposten, «Liten dings skaper store endringer» [«Little doodahs cause big changes»], 16.03.2015, http://www.aftenposten.no/kultur/Liten-dings-skaper-store-endringer-7939980.html

The analysis, «Vil markedsførerne ha behov for markedsanalysis i fremtiden?» ["Will the marketers need market analysis in future?"], Analysis no. 3, 2013, http://www.tns-gallup.no/tns-innsikt/vil-markedsforerne-ha-behov-for-markedsanalyse-i-framtida

Acxiom, «Case study: The Guardian, Boosting audience engagement across the globe», 2014, http://dq2qu0j6xxb34.cloudfront.net/wp-content/uploads/2014/02/The-Guardian.pdf

Adweek, «Google's Latest Role: The Cookie Monster. Ad tech firms are on alert», 11.11.2013, http://www.adweek.com/news/technology/google-s-latest-role-cookie-monster-153712

Article 29 Data Protection Working Party – statements and working documents:

Opinion 2/2010 on online behavioural advertising (WP 171)

Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising (WP 188)

Opinion 02/2013 on apps on smart devices (WP29)

Opinion 03/2013 on purpose limitation(WP29)

Bizreport, «Platform creates customer profiles using Myers Briggs types», 19.04.2012, http://www.bizreport.com/2012/04/platform-creates-customer-profiles-using-myers-briggs-types.htmlSmith

Business Insider, Eric Schmidt: «Google's Policy Is To 'Get Right Up To The Creepy Line And Not Cross It'» 01.10.2010, http://www.businessinsider.com/eric-schmidt-googles-policy-is-to-get-right-up-to-the-creepy-line-and-not-cross-it-2010-10

Business Insider, «Google Is Now Bigger Than Both The Magazine And Newspaper Industries», 12.11.2013, http://www.businessinsider.com/google-is-bigger-than-all-magazines-and-newspapers-combined-2013-11

Calo, Ryan, «Digital Market Manipulation», 82 George Washington Law Review 995 (2014); University of Washington School of Law Research Paper No. 2013-27, 2013, http://dx.doi.org/10.2139/ssrn.2309703

Dagens Næringsliv, «Dette vet mediekjempene om oss» ["The media giants know this about us"], 19.10.2014,

Dagens Næringsliv, «Kjemper om reklamebørs» [«Fighting over ad exchange»], 01.05.2015, http://www.dn.no/etterBors/2015/05/01/2052/Reklame/kjemper-om-reklamebrs

Dagens Næringsliv, «Vil bevise reklameeffekt» [«How to demonstrate the effectiveness of adverts»], 31.07.2015

The Norwegian Data Protection Authority, «Anonymisering av personopplysninger. Veileder, 2015», " [«Anonymisation of personal data. A guide, 2015»], 2015, http://www.the Norwegian Data Protection Authority.no/Global/04_veiledere/anonymisering-veileder-240815.pdf

The Norwegian Data Protection Authority, "Big Data, Personvernprinsipper under press", ["Big Data, principles of privacy under pressure"], 2013, http://www.the Norwegian Data Protection Authority.no/Global/04_planer_rapporter/Big%20Data_web.pdf

Delta Projects, "Nåværende Programmatic status i Norge", ["Current Programmatic status in Norway"], 2014 http://www.deltaprojects.com/assets/programmaticstatusnorway.pdf

The Economist, "Little Brother, Special Report on Advertising and Technology", 13.09.2014, http://www.ogilvydo.com/wp-content/uploads/2014/09/20140913_SR_MAILOUT.pdf

The Council of Europe, "Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling", 2010, https://wcd.coe.int/ViewDoc.jsp?id=1710949

European Data Protection Supervisor, "Privacy and competitiveness in the age of Big Data: The interplay between data protection, competition law and consumer protection in the Digital Economy", 2014, https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2014/14-03-26_competitition_law_big_data_EN.pdf

Federal Trade Commission, "Data Brokers. A Call for Transparency and Accountability", 2014, https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

Financial Times, "How much is your personal data worth?", 12.06.2013, http://www.ft.com/intl/cms/s/2/927ca86e-d29b-11e2-88ed-00144feab7de.html#axzz3lAaLdwax

Gutwirth, Serge and Mireille Hildebrandt, "Some Caveats on Profiling", in Gutwirth, Serge, Yves Poullet and Paul De Hert (eds), *Data Protection in a Profiled World*, pp 31-41, Springer, Dordrecht, 2010

IAB Europe, "An Introduction to Programmatic Trading Webinar", 2014 http://www.iabeurope.eu/files/8914/2789/7694/IAB_Europe_Introduction_to_Programmatic_Webinar_slides.pdf

IAB Europe, "Programmatic Trading. An IAB Europe White Paper"2014, http://www.iabeurope.eu/files/8614/0776/0957/IAB_Europe_Programmatic_Trading_White_Paper_July_2014_v2.pdf

Le Monde Diplomatique, "Reklamerevolusjonen" ["The advertising revolution"], November 2013, http://www.lmd.no/?p=13010

McCafferty&co, "European Media Conglomerate RTL Group Purchases SpotXchange, Paving the Way for Broadcasters to Keep Traditional Ad Dollars without the Traditional Ad Model", 01.03.2015, http://mccaffertyco.com/european-media-conglomerate-rtl-group-purchases-spotxchange-paving-the-way-for-broadcasters-to-keep-traditional-ad-dollars-without-the-traditional-ad-model/

MIT Technology Review, “Navigating Planet Ad Tech. A guide for Marketers”, 2013, http://www.technologyreview.com/campaign/digilant/2014/assets/Navigating-Planet-Ad-Tech.pdf

de Montjoye, Yves-Alexandre, César A. Hidalgo, Michel Verleysen and Vincent D. Blondel, “Unique in the Crowd: The privacy bounds of human mobility”, Scientific Reports 3, Article number: 1376, 2013, http://www.nature.com/articles/srep01376

The New York Times, "When Algorithms Discriminate", 9.7.2015, http://www.nytimes.com/2015/07/10/upshot/when-algorithms-discriminate.html

Olejnik, Lukasz, Tran Minh-Dung and Claude Castelluccia, "Selling Off Privacy at Auction", 2013, HAL Id: hal-00915249, https://hal.inria.fr/hal-00915249

Ot.prp. no. 92 (1998-1999) om lov om behandling of personopplysninger [about the act on processing personal data]

Pando, "Al Gore says Silicon Valley is a 'stalker economy'", 11.06.2014, https://pando.com/2014/06/11/al-gore-says-silicon-valley-is-a-stalker-economy/

Pasquale, Frank, "The Black Box Society. The Secret Algorithms That Control Money and Information", Harvard University Press, Cambridge, MA, 2015

Polakiewicz, Jörg, "Profiling – the Council of Europe's Contribution" in the collection of articles "European Data Protection: Coming of Age", Ed: Gutwirth, Serge, Ronald Leenes, Paul de Hert and Yves Poullet, Springer, Dordrecht, 2013

Rao, A., F. Schaub and N. Sadeh, "What do they know about me? Contents and concerns of Online Behavioral Profiles", Carnegie Mellon University, 2014, https://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab14011.pdf

Smith, Mike, "Targeted. How Technology Is Revolutionizing Advertising and the Way Companies Reach Consumers", Amacom, 2015

Sørgard, Lars, "Informasjonsasymmetri og konkurransepolitikk" ["Information asymmetry and competition policy"], published in: Stortingsmelding [Norwegian parliamentary report] no. 15 (2004-2005): Om konkurransepolitikken [About competition policy], Appendix 1, p 95-109, Department of Economics, The Norwegian School of Economics, Bergen, 2005

TechRepublic, "Windows 10 violates your privacy by default, here's how you can protect yourself", 4.8.2015, http://www.techrepublic.com/article/windows-10-violates-your-privacy-by-default-heres-how-you-can-protect-yourself/

Tran, Minh-Dung, Gergely Acs and Claude Castelluccia, "Retargeting Without Tracking", INRIA, 2015, France,

Turow, Joseph, Michael Hennessy and Nora Draper, "The Tradeoff Fallacy, How Marketers Are Misrepresenting American Consumers And Opening Them Up to Exploitation", Annenberg School for Communication, University of Pennsylvania, 2015, https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf

Turow, Joseph, "The Daily You. How the New Advertising Industry Is Defining Your Identity and Your Worth", Yale University Press, New Haven and London, 2011

USA Today, "Google may ditch 'cookies' as online ad tracker", 17.09.2013, http://www.usatoday.com/story/tech/2013/09/17/google-cookies-advertising/2823183/

The Wall Street Journal, "What they know. The Web's New Gold Mine: Your Secrets", 30.07.2010, http://www.wsj.com/articles/SB10001424052748703940904575395073512989404

The Wall Street Journal, "Websites Vary Prices, Deals Based on Users' Information", 21.12.2012, http://www.wsj.com/articles/SB10001424127887323777204578189391813881534

World Federation of Advertisers, "WFA guide to Programmatic Media. What Every Advertiser Should Know about Media Markets", 2014, http://www.wfanet.org/media/programmatic.pdf

Zuiderveen Borgesius, Frederik J., "Behavioural Sciences and the Regulation of Privacy on the Internet", draft chapter of the book "Nudging and the Law - What can EU Law learn from Behavioural Sciences?", ed. A-L Sibony & A. Alemanno (Hart Publishing), Institute for Information Law Research Paper No. 2014-02, Amsterdam Law School Research Paper No. 2014-54, 2014, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2513771

Zuiderveen Borgesius, Frederik J., "Personal data processing for behavioural targeting: which legal basis?", International Data Privacy Law, pp. 1-14, 2015, http://idpl.oxfordjournals.org/content/early/2015/06/23/idpl.ipv011.full.pdf+html

Appendix 1: Overview of third-party Norwegian online newspapers

The survey was conducted on 4 September and 7 September 2015.

	Aftenposten	Dagbladet	Nettavisen	Adresse-avisen			Dagsavisen		Drammens tidende
Approximate number of third parties	40	43	69	37			36		48
Approximate number of servers the user's IP address is sent to	56	50	84	57			48		61
Approximate number of cookies placed	114	115	196	139			92		156
Analysis	AT Internet Burt Google analytics MixPanel New Relic Rich TNS	Google analytics Hotjar Integral Adsciense TNS	Google analytics Net Ratings SiteCensus TNS	Burt Google analytics Media innovation group Rich TNS			TNS		Google analytics Net Ratings SiteCensus TNS

Marketing	Adform	Adform	[x+1]	Adform			Adform		[x+1]
	Admeta	Admeta	Acuity Ads	Admeta			Admeta		Adap.tv
	AdScale	AdScale	AdAction	AdScale			AdScale		Adform
	ADTECH	ADTECH	Adap.tv	ADTECH			ADTECH		Adition
	AppNexus	Advertising.com	Adform	AppNexus			AppNexus		Adnologies
	BidSwitch	AooNexur	AdGear	BidSwitch			BidSwitch		ADTECH
	Criteo	Bid Swch	Adition	Criteo			Criteo		Advertising.com
	Datalogix	Casale Media	Admeta	cXense			cXense		AppNexus
	DoubleClick	Criteo	AdScale	Datalogix			Datalogix		Brandscreen
	Emediate	Datalogix	Adscience	DoubleClick			DoubleClick		BrightRoll
	Facebook exchange	DoubleClick	ADTECH	Facebook Exchange			Emediate		Casale Media
	Improve Digital	Facebook exchange	Advertising.com	Google Adsence			Facebook exchange		cXense
	Internet Billboard	Google Adsense	AppNexus	Improve Digital			Google Adsense		Datalogix
	LiveRail	Improve Digital	BidSwitch	Internet Billboard			Improve Digital		DoubleClick
	MediaMath	Internet Bilboard	BrightRoll	LiveRail			Internet Billboard		Emediate
	Pubmatic	LiveRail	Casale Media	MaxPoint Interactie			LiveRail		eyeview
	Right Media	MediaMath	Connexity	PubMatic			MediaMath		LiveRail
	Rubicon	Pubmatic	Criteo	Right media			Pubmatic		MediaMath
	Smart Adserver	Quantcast	cXense	Rubicon			Right Media		Moat
	Trade Desk	Right Media	Datalogix	SMART Adserver			Rubicon		Netseer
	Turn Inc	Rubicon	DataXu	Turn Inc.			Smart Adserver		Nexage
	Videoplaza	Smart Adserver	Digilant	Videoplaza			Trade Desk		OpenX
	Yieldlab	Trade Desk	DoubleClick	Yieldlab			Turn Inc		Platform161
		Turn Inc	Dstillery				Yieldlab		PubMatic
		Yieldlab	EQ Advertising						Right Media
			eyeReturn						Rubicion
			Facebook exchange						Smato
									spotXchange

			Google Adsense Improve Digital Internet Billboard LiveRail MediaMath Nexage Nugg.Ad OpenX Platform161 PubMatic Quantcast Right Media Rubicion Smato SMART Adserver spotXchange Tapad The ADEX Trade Desk Turn Inc Yieldlab						Tapad Trade Desk Turn Inc
Privacy							TRUSTe Notice		
Web beacons **(for collecting information)**	Aggregate knowledge Audience Science	eXelate Eyeota Linkpulse	Aggregate knowledge BidTheatre BlueKai	eXelate Eyeota LiveRamp			BidTheatre EXelate Eyeota		Aggregate knowledge Audience Science

	EXelate Eyeota LiveRamp Media optimizer Neustar Adadviser Optimizely Semasio	LiveRamp Media optimizer Neustar Adadviser Optimizely Rhytmxchange Rocket fuel Veruta	eXelate Eyeota Linkpulse LiveRamp Magnetic Media Optimizer Netmining Neustar Adadviser Rocket fuel ScoreCard Research beacon Semasio Videology	Media Optimizer Neustar Adadviser			LiveRamp Media optimizer Neustar Adadviser Videology		BlueKai Chango Linkpulse LiveRamp Media Optimizer Neustar Adadviser Rocket fuel ScoreCard Research beacon Videology
Widgets Social **(Tool for adding content)**	AddThis	Facebook coneckt Facebook Social plugins Google tagmanager Twitter Button	AddThis Facebook connect Twitter button	AddThis Facebook coneckt			Facebook coneckt Facebook social graph Facebook Social plugins Twiiter Badge		AddThis Facebook social graph
Has information been disclosed about how third parties process visitors' personal data?	Generell overordnet informasjon. Ikke noe konkret om 3.-parters bruk.	Generell overordnet informasjon. Ikke noe konkret om 3.-parters bruk.	Generell overordnet informasjon. Ikke noe konkret om 3.-parters bruk.	Generell overordnet informasjon. Ikke noe konkret om 3.-parters bruk.			Ingen		Generell overordnet informasjon. Ikke noe konkret om 3.-parters bruk.

We used the Ghostery analysis tool to find out which third parties were present on the pages.

The newspapers' privacy statements

Aftenposten: https://kundeportal.aftenposten.no/privacy/

Dagbladet: http://www.dagbladet.no/2009/08/18/nyheter/avtale/useravtale/plikter/7706966/

Nettavisen: http://www.nettavisen.no/vilkaar.html and http://www.nettavisen.no/datapolicy.html

Adresseavisen: http://www.polarismedia.no/datapolicy.jsp

Drammens Tidende: http://www.dt.no/tilgang/privacypolicy/

Dagsavisen: Could not find information on the landing page about the processing of personal data.

Appendix 2: Description of third-party players present on Norwegian websites

The descriptions were taken from the websites of the individual companies in September 2015.

AddThis
"The AddThis Audience Intelligence (Ai) platform transforms the real-time activity of 1.9 billion web visitors across 15 million sites into actionable tools to help you optimize your marketing and develop authentic audience relationships."

Adform
"Adform is a cloud technology built for agencies and advertisers, who want to make display advertising the best performance channel by use of personalized targeting, real time bidding and rich media."

Admeta
"Admeta is a company focused on delivering full service technology solutions for large online publishers helping them increase yield on online ad inventory. We are one of Europe's leading suppliers of online ad exchange solutions and are working with some of Europe's largest premium publishers."

Adscale
"Adscale is Germany's leading marketplace for digital advertising, bringing advertisers and website operators together to buy and sell video, display and text advertising."

AdSniper
"AdSniper is an automatic ad placement system, modifying costs in real-time according to the changes in the campaign results." Translated by AdSniper LLC

Adtech
"The company's flagship product is an integrated ad serving platform - amended by features for mobile devices and video ads. These enable web publishers to manage, serve and evaluate virtually any kind of online advertising campaigns. ADTECH allows its customers to enhance efficiency, reliability and ROI in their online advertising businesses."

AppNexus
"AppNexus is the world leader in real-time advertising technology, serving the largest and most innovative companies in the ecosystem on both the buy and sell side. AppNexus offers the industry's most advanced display advertising platform to empower companies to build, manage and optimize their entire display advertising businesses."

AT Internet
"AT Internet is an independent and trustworthy company that enables an integral analysis of websites, intranet and mobile sites."

AudienceScience
"Manage all of your data and digital media in one advertiser-owned SaaS based system with complete control, transparency and efficiency across your entire ad spend. The AudienceScience® Helios technology combines control and ownership of data with 100% media spend transparency. This enables advertisers to store and analyse BIG data, build proprietary audiences, target those audiences across display, video and mobile—in real time—and all within a single, fluid system. Advertisers can now fully and seamlessly manage both their data and buying in one system, enabling safe and effective targeted advertising."

BidSwitch
"IPONWEB has a vision for RTB and Media Trading that is open, transparent and allows many different kinds of businesses to trade and sell media in real-time... Operating as an infrastructure-level 'Switch', the BidSwitch facilitates both Supply and Demand technology partners to efficiently and transparently connect, trade and manage multiple RTB partners."

Burt
"Burt creates software to help advertisers and agencies improve the efficiency and effect of their online campaigns."

Criteo
"Criteo's advanced technology enables online e-commerce sites to re-engage with potential customers who have left their website via dynamic banners containing the most relevant product specific recommendations that are generated in real-time for each individual."

Datalogix
"Even as consumers spend more and more time online, over 85% of purchasing still occurs offline. DLX is the first company to connect the online and offline silos. The result is a first-time, precise digital ROI metric. Now, DLX partners in CPG, Automotive, and Retail verticals have the ability to measure the impact online advertising campaigns have on sales across channels."

DoubleClick
"Google's DoubleClick products provide ad management and ad serving solutions to companies that buy, create or sell online advertising."

Emediate
"Emediate is the leading provider of ad serving technology in the Nordic region."

eXelate
"We make the process of accessing online audiences simple, safe, and scalable by arming data buyers and data owners with proprietary technology that automates data connections and centralizes audience management. Through our DataLinX data management platform, we enable transparent, secure, private data connections for publishers, data owners and marketers."

Eyeota
"Eyeota is an audience-targeting data technology company and the leading source for 3rd party audience targeting data for advertisers across Asia-Pacific, Europe and Australia... Eyeota's solutions are driven by strong, proprietary, data management platform (DMP) and marketplace technologies. Eyeota supplies 3rd party data to all major global and regional ad buying platforms, DSPs and ad networks."

Facebook Connect
"Build with the Open Graph. Integrate deeply into the Facebook experience. Grow lasting connections with your users."

Facebook Exchange
"Through Facebook Exchange, advertisers and agencies have been able to use cookie-based targeting through Demand-Side Platforms (DSPs) to reach their audience on Facebook with more timely and relevant messages. For brands and agencies, the result is a powerful tool for driving direct response goals on Facebook."

Facebook Social Plugins
"Social plugins are tools that other websites can use to provide people with personalized and social experiences. When you interact with social plugins, you share your experiences off Facebook with your friends and others on Facebook."

Google AdSense
"Many websites, such as news sites and blogs, join the Google Display Network, which enables Google to show ads on their sites. Based on your visits to these websites, Google uses an advertising cookie (from DoubleClick) to associate your browser with interest and demographic categories. Google then uses these categories to show interest-based ads on these websites. Google's Ads Preferences Manager lets you edit these categories associated with your browser. Using the Ads Preferences Manager, you can edit the list of inferred interest and demographic categories that Google has associated with your cookie or opt-out of the cookie entirely. All information Google gathers is used in accordance with Google's privacy policy and helps Google improve your online experience. It is not used to identify you personally and Google will not show interest-based ads based on personal information without your permission. We also will not show interest-based ads based on sensitive information or interest categories, such as those based on, race, religion, sexual orientation, health, or sensitive financial categories, without your opt-in consent."

Google Analytics
"Google Analytics gives you insights into your website traffic and marketing effectiveness. We help you buy the right keywords, target your best markets, and engage and convert more customers."

Google Tag Manager
"Google Tag Manager is free and easy, leaving more time and money to spend on your marketing campaigns. You manage your tags yourself, with an easy-to-use web interface, rather than forcing you or your IT department to write or rewrite site code."

Improve Digital
"The company provides real time advertising technology to owners of premium digital media that want to build their own Private Ad Ecosystem. Improve Digital enables them to build, grow, manage, control, and optimise their own environment driving revenues from direct campaigns, RTB, ad networks, exchanges, trading desks and any other 3rd party media buyer."

Internet Billboard
"The Internet BillBoard company develops and runs software solutions for a complex internet advertising management and runs the biggest internet advertising network in the Czech Republic and Slovakia. We develop and run the advertising management system BBelements AdServer, BBelements IntextServer and other products."

Linkpulse
"Linkpulse is an analytics tool tailor made for high traffic news sites. Optimize and prioritize your front page backed by live data."

LiveRail
"LiveRail delivers technology solutions that enable and enhance the monetization of internet-distributed video."

LiveRamp
"LiveRamp helps marketers with CRM Retargeting and helps data companies onboard their offline data into anonymous cookies." (LiveRamp, formerly Rapleaf)

Media Innovation group
"We provide marketing communicators with a single access point to every digital audience, and the technology platform to engage them in startling new ways."

Media Optimizer
"Adobe Media Optimizer provides customers the ability to deliver relevant ads to targeted audiences. Our technology provides both data management functionality and a unified campaign management platform that optimizes advertising campaigns across search, display and social."

Mixpanel
"Mixpanel's mission is to help the world learn from their data. We offer the most sophisticated analytics platform companies online can use to understand how users behave. We do all of our data analysis in real-time."

New Relic
"New Relic is the all-in-one web application performance tool that lets you see performance from the end user experience, through servers, and down to the line of application code."

Neustar AdAdvisor
"Our core mission is to provide the most comprehensive, accurate and up-to-date IP geolocation service. If your business is looking to improve your marketing and website's performance, enhance your customers' experience, ensure your customers' online safety or confidently comply with your industry's regulations, Neustar's IP geolocation services are right for you."

Optimizely
"Optimizely, Inc. offers a range of website analytics services for A/B and multivariate testing purposes. Optimizely partners implement Optimizely as a way to better understand how their website is used."

PubMatic
"PubMatic's ad monetization and management solution combines impression-level ad auction technology, the most comprehensive brand protection tools, and enterprise ad operations support to give the Web's premium publishers the most control over their revenue and brand."

Rich
"Rich is the campaign analytics tool used by the world's leading digital agencies and advertisers."

Right Media
"Right Media launched the first global digital advertising exchange in 2005, evolving to support the needs of businesses in today's digital media world. From sellers maximizing yield to buyers optimizing their ROI, businesses choose Right Media as the premium, trusted destination where they can build invaluable relationships."

Rubicon
"Powered by the REVV Yield Optimization Platform, the REVV Marketplace is the world's largest premium display advertising marketplace, providing a single point of access for the over-whelming volume of opportunity that exists for publishers today. From international networks to DSPs to highly niche demand sources, publishers can access it all via the REVV Marketplace, enabling publishers and their sales channels to transact efficiently, effectively and safely."

Semasio
"The User Intelligence Platform enables you to turn all of the potentially hundreds of contacts you have with digital media users into data points from which a qualitatively new level of information is derived – information which belongs to you and only you."

Smart AdServer
"Smart AdServer develops and markets premium ad serving solutions for media agencies and publishers to manage display campaigns for Web, mobile and iPad/tablets."

TNS
"TNS is the world's largest Custom Market Research specialists. We provide quality marketing information delivered by Global Industry Sector expert consultants, innovative Market Research Expertise across the product life-cycle, in 80 countries."

Trade Desk
"We power the most sophisticated buyers in advertising technology."

Turn Inc.
"Turn has developed the digital advertising industry's only integrated, end-to-end platforms for data and media management. The Turn Audience Platform and Turn Media Platform are currently utilized to manage digital advertising campaigns for Global 2,000 brands. Turn's global infrastructure, intuitive software and analytics, and open ecosystem for partners – all available in a real-time integrated environment – represent the future of digital advertising."

Twitter Button
"Twitter is a real-time information network that connects you to the latest information about what you find interesting...At the heart of Twitter are small bursts of information called Tweets. Each Tweet is 140 characters in length."

UserVoice
"UserVoice helps companies listen to their customers to build better products and improve customer satisfaction. We've built a platform that helps companies, from startups to Fortune 500s, collect feedback from thousands, and sometimes millions, of customers."

Videoplaza
"Videoplaza empowers broadcasters, publishers and ad networks to maximise their advertising revenues from the New IP-delivered TV. Videoplaza's sell side ad management platform, Karbon, is used to monetise video experiences across PCs, mobile devices, tablets, game consoles, IPTV and Smart TVs."

Yieldlab
"Our focus is on the development of software systems for the real-time trading and delivery of advertisements via digital channels. We enable web sites, marketers, media houses and publishers, to strengthen and optimize their business relations with agencies and advertising clients."

Appendix 3: Glossary

Ad call
An ad call is a notification which is sent from the newspaper's server to the ad exchange in order to provide notification that a user is in the process of downloading a page on which ad spots have to be filled with content.

Ad exchange
An ad exchange is a marketplace for the purchase and sale of advertising space, built up according to the same principles as with stock exchanges. The ad exchanges are a platform for operating real-time bidding in which purchasers of advertising spaces can bid for users offered by the publishers. On the open ad exchanges (in contrast to the private market places, see below) access is open to all players to buy and sell users side by side (limited access for a few categories of websites, for example pornographic websites).

Ad tag
An ad tag is an ad code linked to the adverts on the page which the user is loading. When this code reaches the user's computer it immediately sends a notification to the ad exchange with which the newspaper has an agreement. The notification which is sent from the newspaper's server to the ad exchange via the user's web browser is called an *ad call*.

Aggregated data
Statistical data about several individuals that has been combined in order to show general trends or values without identifying individuals in the data set. Aggregated data are not necessarily anonymous data.

Anonymisation
Anonymisation is rendering personal data anonymous. Data sets that can be linked to an identifiable person are adapted with a view to making it impossible to link the information and the individual. Several techniques can be used to achieve the goal of rendering the information anonymous.

Anonymous data
Data which it is not possible to link back to an individual using all appropriate technical equipment.

The Article 29 Working Party
The Article 29 Working Party is made up of a representative from the data protection authority of each EU Member State, the European Data Protection Supervisor and the European Commission. Norway has observer status in the group.

Beacon
Beacons are small sensors that use Bluetooth technology to transmit information which can be received when someone comes close to them. Using the technology demands that the user has equipment that can read the information which is transmitted.

Cookie
An information capsule or cookie is a small file that is saved in the user's equipment when the user visits a website. Every time the user visits the website the web browser sends information back to the website's server in order to notify the website about the user's activity on the page. Companies can place cookies that are stored on people's equipment for several years, even for more than 10 years, or use cookies which are immediately deleted when the web session finishes.

Cookie matching
Cookie matching is a crucial functionality in association with real-time bidding for unique users on exchanges. In order for those on the purchasing side to be able to decide whether they want to submit a bid, and not least how much they will bid, they must know who the user is. Cookie-matching makes it possible to link data which are in the database to the vendor and to the buyer of the user.

Data Management Platform
Data Management Platforms (DMP) are data warehouse technology which is used to organise, align and analyse data from many different sources. The objective of a DMP is to put data together in such a way that it produces the richest

possible understanding of the individual consumer.[114] The objective is to help marketers and publishers understand their customers better. It is used to segment and profile the customer base.

Demand Side Platform
A demand side platform is software which has been specially developed to purchase users on the ad exchanges. A demand side platform purchases users based on targeting criteria (an algorithm) developed in partnership with the advertiser. The algorithm is based on aligning first-party data and data gathered from other sources.

IP address
An IP address is a unique identifier which points to a device, such as a PC or a tablet, in a network such as the Internet.

Personal data
Is a piece of information or an assessment which can be linked to you as an individual

Private Market Place
A private market place is an ad exchange controlled by publishers where they put users up for sale to invited demand side platforms.

Profile
A profile is made up of assumptions about the preferences, abilities or needs of an individual or a group of individuals. The assumptions are derived from measures which include an analysis of individuals' browsing history, updates on social media, news articles read, products bought on the Internet and registered customer information. Assumptions are also regarded as personal data, even though they are not actual information.

Pseudonymisation
A process in which directly identifying parameters are replaced by unique indicators in order not to directly reveal the true identity of the data subject.

Real-time bidding
System for buying and selling users in real time on ad exchanges. The system makes it possible for purchasers of advertising space to estimate the value of, and submit bids for, unique users offered by publishers. The advert buyer who submits the highest bid for the user wins the right to show the person concerned an advert on the website which is loaded.

Re-targeting
Re-targeting is a term for when advertisers show advertising for a product which they know the customer has already seen. For example, they may wish to show adverts for shoes to a user who they know has looked at shoes or has previously been exposed to shoe adverts.

Sensitive personal data
Information about racial or ethnic background, or political, philosophical or religious views, the fact that someone has been suspected of, charged, prosecuted or convicted of a criminal offence, or health conditions, sexual orientation or membership of trade unions.

Supply Side platform
A supply-side platform is software which has been developed to offer vacant ad spots and users for sale on ad exchanges.

Web beacon
A web beacon is used on its own or in combination with cookies to obtain more information about the visitors to a website. A web beacon is usually an invisible graphic image (usually 1 pixel x 1 pixel) which is placed on the website. Web beacons are also used by third parties to gather information about the users and as a mechanism for placing

[114] IAB Europe, «Programmatic Trading. An IAB Europe White Paper», 2014, http://www.iabeurope.eu/files/8614/0776/0957/IAB_Europe_Programmatic_Trading_White_Paper_July_2014_v2.pdf

cookies. Web beacons can be used to gather information about the user's IP address, the time when the website was visited, which web browser the user has and more.

Datatilsynet

Besøksadresse:
Tollbugata 3, 0152 Oslo

Postadresse:
Postboks 8177 Dep., 0034
Oslo

postkasse@datatilsynet.no
Telefon: +47 22 39 69 00

datatilsynet.no
personvernbloggen.no