

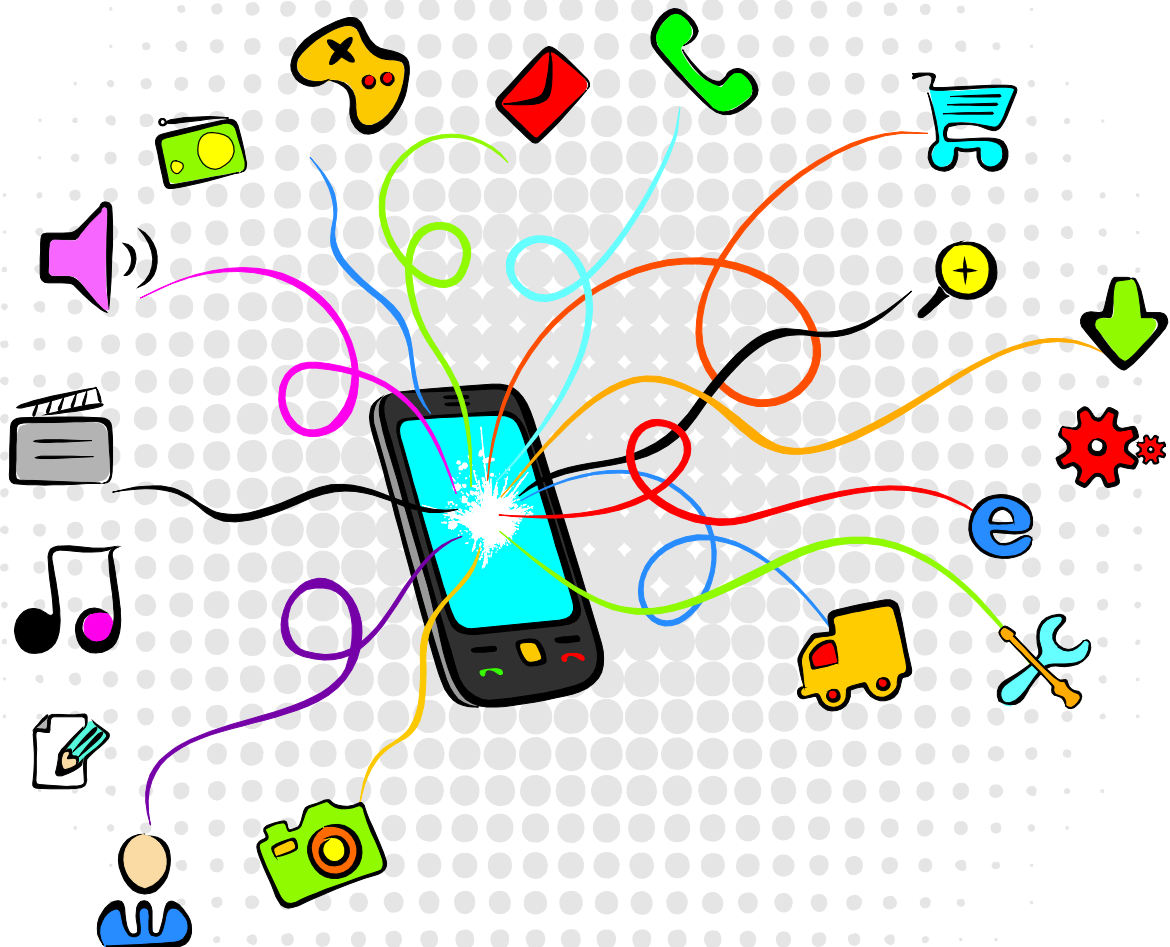


Datatilsynet

What does your app know about you?

Data protection challenges in the mobile applications market

Atle Årnes and Catharina Nes,
September 15th, 2011



Executive summary

Mobile applications, or 'apps', are a fast growing market. Hundreds of thousands of applications are available to download from a range of 'app stores'. Apps are funny, practical and easy to use; but many apps also collect large amounts of personal details about their users, often without users being aware of this.

As far as the users are concerned, the app market is largely non-transparent when it comes to *which* data is collected about users, *why* it is collected, and *how* it may be *reused*.

When downloading an app, users have to determine whether they believe their personal data will be handled acceptably. As the information to users on how their personal data is handled is patchy, they have to trust the individual app providers when engaging in these transactions. iPhone users leave the processing of their personal data to Apple, which approves all apps in advance and thus guarantees that they meet certain requirements. From a user's perspective, we can compare how the iOS platform handles personal data to opening a *huge door* into the phone. Once this door is open, users have no way of knowing exactly what information passes through it and have to rely on Apple having full control over apps and what they can take.

How Android process personal data can be illustrated with opening a number of *small holes* into the phone. Once these holes are open users have little control over what goes through them. There is no authority to supervise this. Users may end up installing applications that allows access to information on the mobile they do not want to share. Compared with iPhone users, Android users can make a slightly more qualified assessment of any given app before downloading it; but they still have to base the installation on trust.

In the app market, it is very hard to define who is legally responsible for what, and there are many different players involved. The key players, apart from the end users, are mobile phone providers, operating system providers, app providers, app developers, app clients and various third parties such as analysis companies and market researchers. The legal responsibility for an application must be established in each separate case, with reference to the purpose for collecting personal data and contractual relationships between the parties. Those legally responsible have amongst other things a duty to disclose how they process personal data.

The right to be informed about and also to see how one's personal data is processed are important principles of data protection. None of the Norwegian applications that the Data Inspectorate has looked at provide easily available information to users about how they process personal data once they are collected. The possibility for providing information on how apps handle personal data in the App Store or Android Market is rarely used. Had this option been used more, users would have been given a better basis to decide whether to install an app or not before doing so. Nor is there much information to users on how the apps handle personal data within the app itself. It would be useful to provide information here too so that users are able to easily access this information also after downloading apps. And, finally, it is essential that the entity legally responsible for the apps state on their website how each one of the apps handle personal data. They rarely do so. However this is an important channel to communicate information about who is liable for the apps and which jurisdiction is relevant.

Contents

- Executive summary 2
- 1 Introduction..... 5
- 2 The mobile application market in brief 7
 - 2.1 What is an 'app'? 7
 - 2.2 Apple vs. Android 7
 - 2.2.1 Apple - iOS 7
 - 2.2.2 Android 8
 - 2.3 Who is hiding behind an app? 8
 - 2.3.1 Applications developers 9
 - 2.3.2 App clients (app owners)..... 9
 - 2.3.3 Third parties 9
 - 2.3.4 Operating system providers and app providers 10
 - 2.3.5 Mobile operators..... 10
 - 2.3.6 Mobile phone providers 10
- 3 What do apps know about you? 12
 - 3.1 What information do apps extract? 12
 - 3.1.1 Location data 14
 - 3.1.2 ID data 15
 - 3.1.3 Contact data 15
 - 3.1.4 Calendar data 16
 - 3.1.5 Cameras and microphones..... 16
 - 3.1.6 Gyroscope and accelerometer 16
- 4 Lack of transparency 17
 - 4.1 System based on trust 17
 - 4.2 Absence of information..... 17
- 5 Who is in charge? 19
 - 5.1 A data controller must be identified 20
 - 5.1.1 Relations between developers and clients..... 20
 - 5.1.2 Dealings with third parties 21
- 6 Other legal issues 22
 - 6.1 A contract is the foundation..... 22
 - 6.2 Rights of inspection and information 22
 - 6.3 Relations with other legislation..... 23

7	Conclusion	24
8	ANNEXES.....	25
	Annexe 1: Norwegian Android apps studied in report.....	25
	Annexe 2: Foreign Android apps studied in report.....	26
	Annexe 3: List of questions sent to Norwegian app developers.....	27
	Annexe 4: Typical information page on Android Market.....	28
	Annexe 5: List of data elements apps need access to.....	29
	Annexe 6: Norwegian apps with data protection statements	30

1 Introduction

Mobile phone applications or 'apps' are a fast growing market. There are hundreds of thousands of applications to download, from different 'app stores'. Apps are fun, practical and easy to use – you can check the weather, play games, or find out when the next bus goes, just by pressing a button. But many apps also collect large amounts of personal details about their users, often without users themselves knowing. Some apps require access to personal details that can tell a lot about you, like where you have been in the last few days, who your friends are and what you are interested in.

A recent survey of US smart phone users found 38 % said protecting themselves was their main concern when using mobile apps¹. Nearly everyone who was surveyed said they wanted more transparency in dealing with personal data and control over what that data is used for. People were concerned about what data apps actually collect and how marketers and others might use that data. Why would a 'pocket light' app need to access a phone's identity, for example?

Personal data is a rapidly growing commodity. Apps are often free or very cheap: the real currency is often the personal data you reveal. Personal data is attractive to analysts, marketers and advertisers: the more information they manage to collect on users, the better they can tailor advertising to consumers.

Telling the users which personal data is collected, why it is collected and how that data is treated is essential in order to have proper data protection. The reason the Data Inspectorate is focusing on the app market is that we have the impression that users are largely uninformed about what personal data is being collected, and that it is not clear who is legally responsible amongst those involved. Who is responsible for ensuring personal data is handled correctly: is it those who order apps, those who develop them, those who supply them, or the app users themselves?

The Data Inspectorate's report aims to discover how mobile applications collect personal data from smart phones. This report also looks at responsibilities in the app market and to what extent apps come with a data protection policy. The Data Inspectorate has not investigated how the collected data are being processed by app-owners and whether and how it is reused by third parties: this is a problem the Agency may look at in more detail in a subsequent report.

The Data Inspectorate's report looks at applications developed both in Norway and abroad, but the focus is mainly on the Norwegian market. The report covers applications developed for the two main platforms, Android and Apple / iOS; it does not discuss data protection problems relating to the operating systems themselves.

¹ No equivalent studies have been conducted in Norway. The US survey was conducted by TRUSTe, a leading supplier of online data protection solutions http://www.truste.com/about_TRUSTe/press-room/news_truste_mobile_privacy_survey_results_2011.html

Methodology and resources

The contents of the report are based partly on our own empirical investigations and partly on outside source material. The Data Inspectorate has taken a closer look at twenty Norwegian and twenty foreign Android applications, aimed at discovering what data on mobile phones applications need access to and whether those applications come with a privacy policy. The Agency selected some popular Norwegian and foreign applications in different fields (games, navigation services, weather services, food services, news, banking, etc.)

The Data Inspectorate has only used publicly available information in its report, focusing on the user's perspective and what information is available to users when they come to download apps. The aim of the report has not been to '*discover*' what data apps might collect on the quiet.

Initially, the Data Inspectorate aimed to look into applications on *both* the two most popular platforms. Android applications come with a relatively detailed list of what data elements they need to access on phones: it is this list we used in our analysis. The iOS platform, on the other hand, is more 'closed' than Android, and what data Apple apps need access to is not publicly available: so we have only studied Android applications in this project.

"*The App Genome Project*"² conducted by Lookout Mobile Security has conducted surveys into both platforms, and has examined 500,000 apps to date. They conclude that both Android and iOS applications take a volume of personal data which is more or less equal: we therefore believe that analysing Android apps alone will still give a relatively good indication of how much applications collect data *generally* independent of the platform involved. The apps were studied in September 2011.

The Agency has also spoken with Norwegian mobile application developers. The report does not name these companies, as the focus was not on specific companies or applications. The purpose of the discussions was to find out more about apps and get some insight into how they are developed and hear what development environments think about data protection problems. These discussions were held in May - June 2011.

²*The App Genome Project* is the world's most comprehensive analysis of mobile applications, and aims to find out how applications go about identifying different potential security threats. The project is still in progress, and had examined 500,000 Android and iOS applications by February 2011. Lookout Mobile Security is a company that makes security solutions for smart phones. <https://www.mylookout.com/appgenome/>

2 The mobile application market in brief

2.1 What is an 'app'?

It is the spread of smart phones in particular that is driving the app market. The electronic industry foundation [Stiftelsen Elektronikkbransjen] has estimated that 70 % of all new mobile phones sold in 2011 will be smart phones³. In other words, using applications is no longer a niche activity reserved for young technology geeks, but something broad strata of the population use on a daily basis.

Smart phones are mobile phones that offer more advanced data processing and better connections than conventional mobile phones. In fact, smart phones are small handheld computers, on which small programs, or applications – popularly known as apps – can be installed.

Smart phones come with different operating systems, and applications are developed specifically for those systems. Other operating systems as well as Apple's iOS and Google's Android is Microsoft's Windows Mobile, Symbian from Nokia and RIM's BlackBerry⁴.

Apps are available via the different platforms' app stores, the top two being Apple's App Store and Google's Android Market. The number of apps available from these stores is growing enormously: Apple has approved 500,000 apps for sale at its App Store, while around 300,000 apps are available on the Android Market⁵. Ten billion apps had been downloaded from App Store as at January 2011⁶.

Foreign applications dominate the list of popular apps at Android Market and App Store, but popular Norwegian apps are coming increasingly on to the market. Some typical much used Norwegian apps are VG, Trafikanten, MatPrat, GuleSider [Yellow Pages], Wimp, Norsk TV guide and Norsk Tipping.

2.2 Apple vs. Android

Android and Apple have very different profiles. Apple's iPhone and its associated operating system is a closed system in which Apple approves everything from hardware to content and the software available: the Android system, on the other hand, is open, and manufacturers are free to design their own phones, and the content is user driven, free and without prior approval.

2.2.1 Apple - iOS

Apple maintains strict control over what applications are offered. Each and every application must meet the requirements that Apple has laid down and lays down under its contracts. That means it checks and approves all applications that are offered. Users must accept Apple's terms and conditions before they can use the App Store. These terms and conditions are universal, and apply to all applications offered via the App Store generally⁷.

³ <http://www.aftenposten.no/forbruker/digital/nyheter/mobil/article4085155.ece>

⁴ RIMs BlackBerry is not widespread in Norway, but is the most widely used smart phone in the USA

⁵ Figures from May 2011. <http://www.nrk.no/vitenskap-og-teknologi/1.7650781>

⁶ <http://www.digi.no/861028/over-60-apps-lastet-ned-per-ios-enhet>

⁷ Apple allows applications aimed at specific closed groups, such as staff at a company, to have customised solutions; but such applications are handled quite strictly, so no one outside can use them. Such 'business' applications do not come under Apple's regime for approving applications.

iPhone users can bypass Apple's restrictions when it comes to applications, by using what is known as a jail break on their phones. 'Opening' an iPhone like this is a matter for those specifically interested, and will not be considered any further in this report.

It is basically impossible for an iPhone user to see what data apps take from their phones. In theory, any application can access anything; but Apple's approval procedure should prevent the application from making any unwanted retrieval of information. As Apple's approval procedures are based on the contracts that Apple uses, and not on European or Norwegian data protection legislation, it is difficult for users to have a clear idea of what personal data is collected and used; and the contracts Apple presents to users are extremely comprehensive and impenetrable to the average user. Apple also updates and amends these rules on a regular basis, which makes it hard to know what current practice is at any time.

2.2.2 Android

The Android platform works completely differently from iOS. There are no procedures for approving Android apps (agreement⁸). The Android platform is based on open source code, although anyone developing Android apps must use predefined tools the platform provides. These tools provide access to data on users' phones, but cannot access that data without users knowing. Users are informed when applications are installed, and can then decide whether to install those applications or not. Users cannot exclude individual tools used in an app, it is however possible in some cases to block access to particular data elements the apps want to access, such as GPS, for example.

The Android platform uses what is known as 'sandbox technology': this means each Android app works alone, and cannot access details of other apps installed. It can access to details of other apps via storage areas, such as the SD card, where applications can store significant amounts of data.

2.3 Who is hiding behind an app?

The application market is a highly complex one: the 'ecosystem' apps are involved in involves many different players, on many sides of the globe. Apart from end users, the key players are mobile phone providers, operating system providers, app providers, app developers, app clients and various third parties like analysts, marketers and location service providers.

⁸ <http://www.android.com/us/developer-distribution-agreement.html>

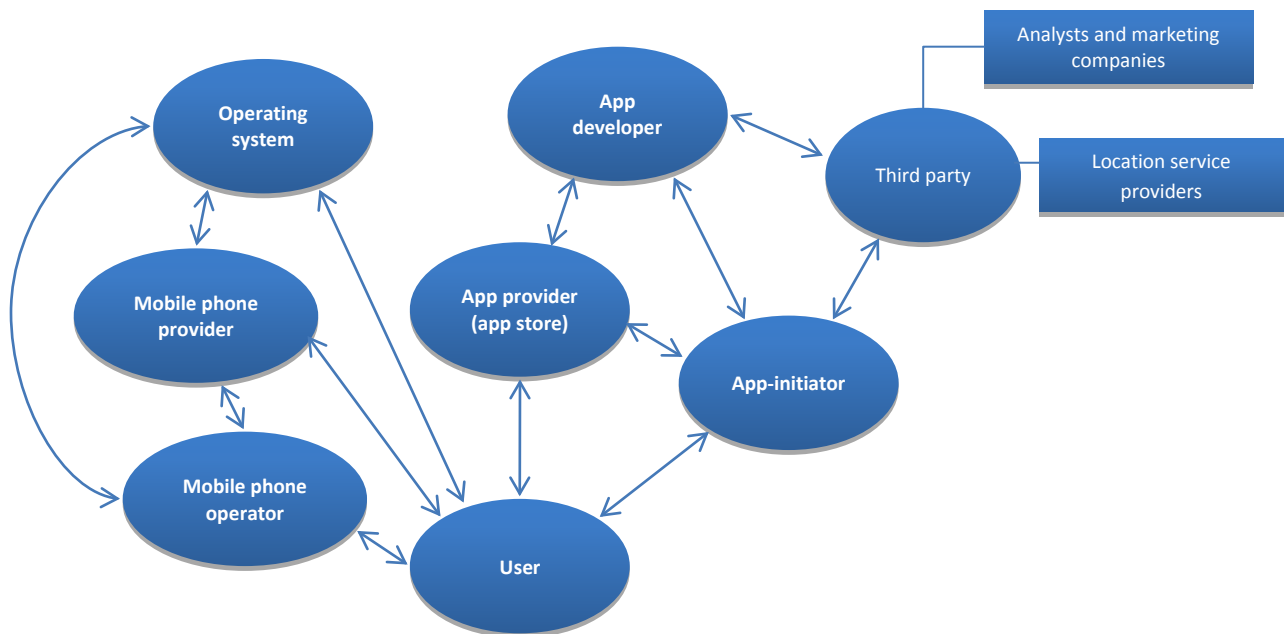


Fig. 1: Players in the 'app ecosystem'

2.3.1 Applications developers

Applications developers write apps. This is a growth industry, with more and more companies offering applications development for iPhone, Android and other platforms.

Many Norwegian companies have appeared offering to develop applications for smart phones and tablets; and already established marketing and internet agencies have set up their own departments to develop apps. Many apps are still being developed by private individuals.

Application developers often write apps jointly with third parties, like analyst companies, location service providers, advertisers and clients.

2.3.2 App clients (app owners)

More and more public and private players are seeing the benefits of offering services and marketing themselves via mobile applications. App clients get in touch with developers to create applications. Companies that have developed popular apps include Trafikanten, Gulesider and VG.

The report will discuss the responsibilities involved between the app developers and the app instigators, which are not clear, in section 5.1.1.

2.3.3 Third parties

Third parties can be divided into many different groups. There are advertising providers, analysis companies, location service providers and others basically offering services to app developers. An analysis of 300,000 apps under the App Genome Project found that 47 % of free apps on Android contained third party code, while the corresponding figure on the iOS platform was 23 %⁹.

⁹ <http://appadvice.com/appnn/2010/07/report-14-percent-iphone-apps-users-contact-information>

Third party code is offered to application developers as free services they can use in their applications for different purposes. In return, third party code providers often get access to analyses, statistics and the like: this information can often be processed and sold on to analysts, marketers and others out to find the right target groups for their products.

The biggest player in this market is *Flurry*. Flurry is an analysis service which helps app developers see how their apps are used. If Flurry is integrated in an app, it will send out detailed information about how that app is used. Information is sent to Flurry's own database, which developers can log into and see statistics for their apps.

According to an article on *Dagensit.no* dated 26 January 2011, the company behind Flurry is sitting on enormous amounts of information on the general public collected from different apps¹⁰. Flurry can, so to speak, monitor all information as to how people use their mobiles. Users are generally not told that Flurry or similar services are included in applications. Responsibility for third party applications is discussed in section 6.1.2.

One thing which emerged when talking with Norwegian app developers is that some companies have concerns about using analysis services like Flurry in their applications. This was partly because they are not certain about how these third party companies use the personal data they collect from Norwegian users. One of the companies that the Data Inspectorate talked to therefore developed its own analysis tool to avoid using Flurry.

2.3.4 Operating system providers and app providers

App providers like App Store and Android Market also collect personal data on users. App Store requires users to enter their credit card numbers, for example, even if they do not intend to buy anything from the store, but are merely using free apps. This can be used to identify users.

Both iPhone and Android offer users apps that are linked to the operating system, that is, apps which are developed by the operating system providers themselves and not by third parties. Operating system providers can include processing personal data in their operating systems, for both their own and others' use. Apps can report location data, for example. Operating system providers provide recipes for avoiding such reporting with some elements (GPS is an element, for example); but it is not clear to customers what kind of personal data is collected by operating system providers' apps, whether it is location data, contact data and so on.

2.3.5 Mobile operators

Mobile operators such as Telenor and Netcom store personal data needed to bill their services. They also process data to maintain security and operate services, which includes location data. Mobile operators are not good at telling users they hold such information. The Data Inspectorate knows that, if users ask to see the processed data, they will normally be given billing data, but not location data.

2.3.6 Mobile phone providers

Mobile phone providers can set up areas of their operating systems to collect personal data themselves, such as reporting location data to the provider and identify data in some cases.

¹⁰ <http://www.dagensit.no/article2066963.ece>

3 What do apps know about you?

“You should know that any data that can be gathered will be gathered”¹¹.

Some data is more sensitive in terms of data protection than others; but any personal data may be perceived as sensitive if combined with other data, even though any one element may not be seen as sensitive in isolation.

Let us take an example: Anne downloads an app from Android Market. This service is a location based social service: Anne can use it to show her friends where she is and get offers from local shops. To locate Anne, this app needs to access the location of her mobile phone. Anne is happy to share her location data with her friends. What she does not know is that this app, which needs access to her contact list on her phone, shares this information with *all* contacts on that list. This app also has an analysis tool which gathers a broad spectrum of different information about Anne. This information is attractive to marketers and others who want to sell products in areas where people with Anne's profile hang out.

To marketers, such information is extremely valuable: the more information they have, the more they can customise their marketing and make it more effective. That means smart phones and apps are valuable 'tools' as far as marketers are concerned, as they can be regarded very much as sensors for conducting detailed market research into the public at large.

3.1 What information do apps extract?

The Data Inspectorate has examined 20 Norwegian and 20 foreign Android applications: the table below is based on information obtained on each individual Android app on Android Market under the 'consents' flag¹². As we saw earlier, Android apps list what data elements on phones they need access to. The tables below show the most key data elements. For a complete list of all data that apps require access to see Annexe 5:

¹¹ “Snooping: It’s not a crime, it’s a feature”, Mark Elgan in Computerworld, 16 April 2011
http://www.computerworld.com/s/article/9215853/Snooping_It_s_not_a_crime_it_s_a_feature?taxonomyId=84&pageNumber=2

¹² See Annexe 4

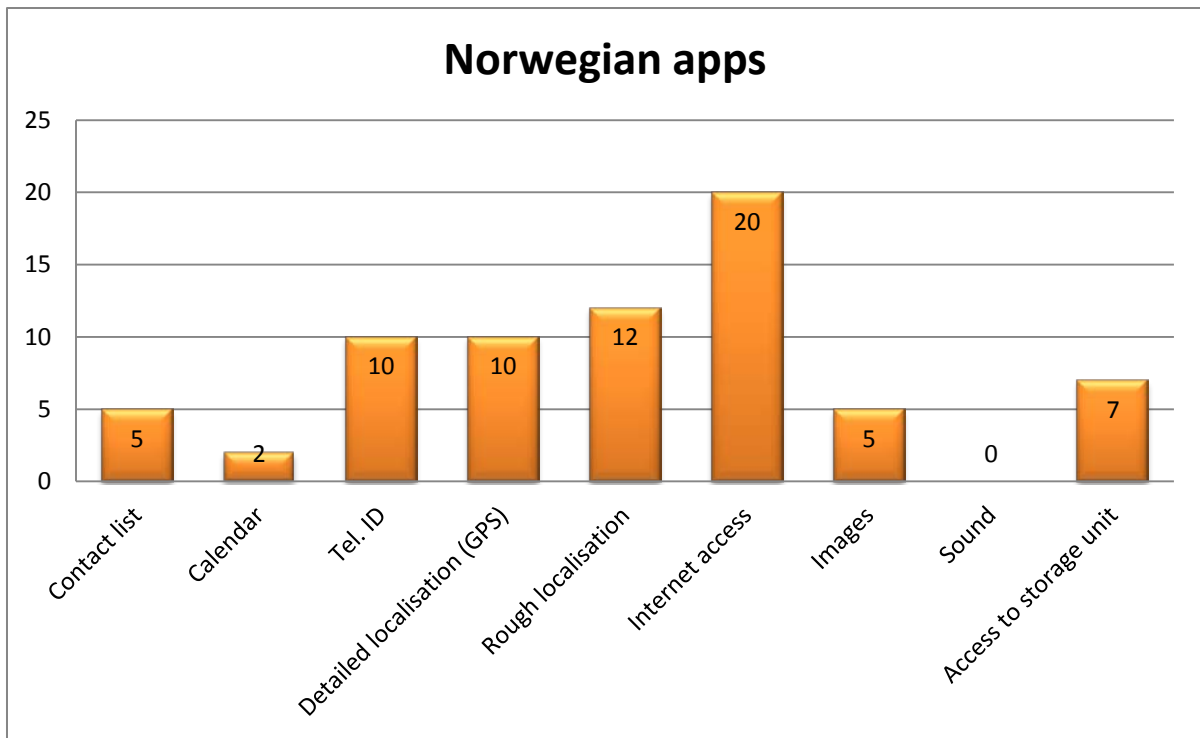


Table 1: List of what data 20 Norwegian Android apps state they need access to

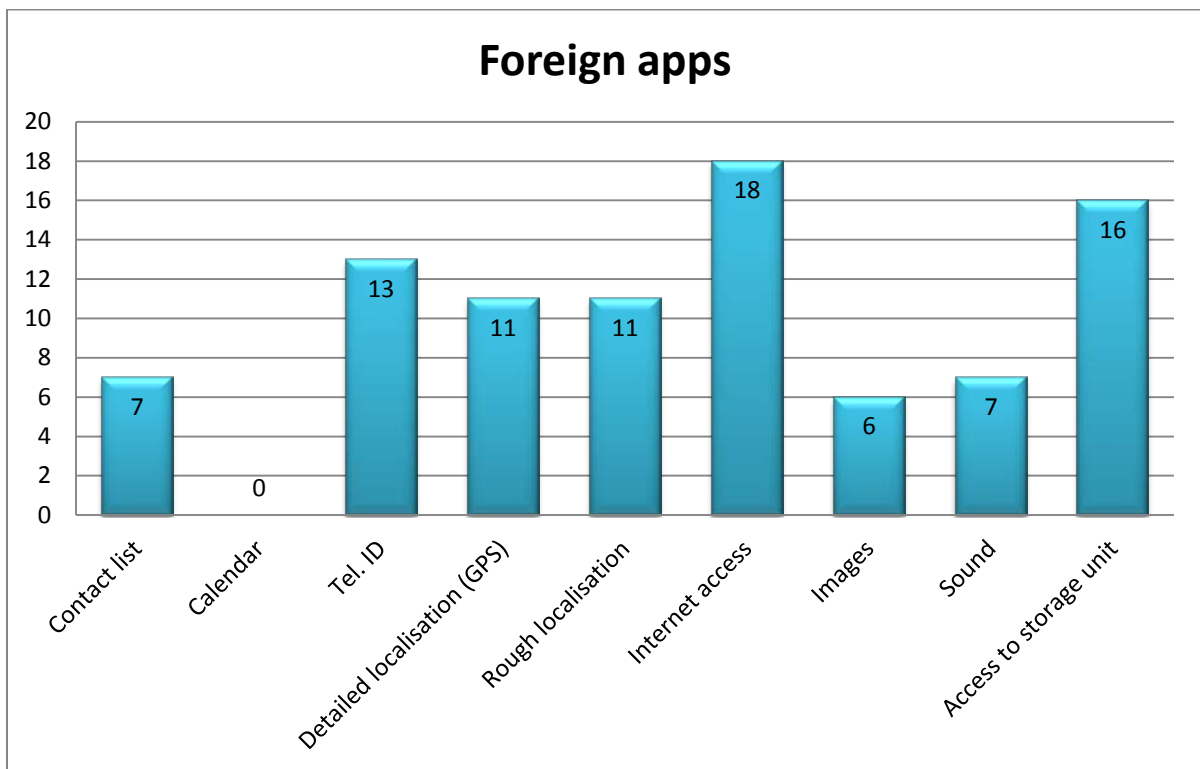


Table 2: List of what data 20 foreign (mainly US) Android apps say they need access to

The data that apps need to access on smart phones can be divided into two main groups: on the one hand, there is data which is held statically on mobiles, and on the other, data that mobile hardware generates continuously (hardware controllers).

Examples of static data held include:

- Identifying data (see 4.1.2)
- Contact data (see 4.1.3)
- Text (unencrypted text, such as notes)

Dynamic data includes such things as:

- GPS, WiFi, base station location (see 4.1.1)
- Camera data (see 4.1.5)
- Microphone sound (see 4.1.5)
- Data from gyroscopes and accelerometers, motion sensors, x, y and z axes (see 4.1.6)

3.1.1 Location data

Location data is an important, much used data component for the different players in the app market. Half the apps we looked at gather such data.

Location data is often regarded as some of the most sensitive data gathered about us. As mobile phones are closely linked to their owners, storing their movement patterns on their phones will give extremely detailed insights into those owners' private lives. We are rarely parted from our mobile phones, so they show where we are just about all the time.

There are at least three ways of collecting location data:

- GPS: gives a highly precise location, accurate to within a few metres
- WiFi: can give very precise location details in highly built up areas, accurate to within less than 100 m.
- Base station data: can give quite precise location data in built up areas, accurate down to 100 m.

Users can switch the GPS and WiFi element off; but base station data is harder to switch off, as it would prevent using a mobile to communicate normally.

On the iOS platform, GPS location can be switched off for individual applications; but users are not told whether this also prevents using IP location via WiFi or location via base station. On the Android platform, GPS data can be switched off generally, but the same questions then apply as with iOS, whether users can be certain that using IP location via WiFi or location via base station is also excluded. As far as the Authority know there is not possible for the user to be protected against that none of the various options for localization are being used; nor are they told how the collected data is used and possibly reused by players in the ecosystem we saw above.

The Art 29 group, which is an association of data protection authorities in the EU, has published its own opinion on location services on smart phones¹³. This document concludes that players who want to use location data must obtain the users' active consent.

3.1.2 ID data

It is usual to ask for ID data to set up communications with app users. ID data is typically name, address, mobile no., email address, IP address, IMEI no.¹⁴, credit card data and account no. Around half of the 40 applications the report examined collect ID data.

Unique user ID data is highly valuable to many players in the app market. Such data is of interest, because it can be used for many other remunerative purposes than its original one. It is extremely valuable when it comes to producing good profiles of customer bases, for example: so there are many players who will have little interest in deleting such data. European law lays down clear requirements on processing this kind of data; US legislation is less clear, however.

Users who use applications that require access to ID data have very little control over how that data is used and possibly passed on by other players as things currently stand.

In the PC market, there has been a high level of awareness on collecting ID data and that it should be possible to avoid using it¹⁵. Norwegian e-commerce rules regulate things like using cookies¹⁶. The app market has not focused likewise on the importance of anonymity to date.

3.1.3 Contact data

Contact data may involve enormous amounts of data elements. Basically, contact data is email address, name and telephone number. It may also include such things as date of birth, job, interests, family and friends. Many applications find it relevant to collect contact data or add contact data on users' smart phones.

The contact data applications take from phones is not limited to app users themselves, but also the contacts they have registered on their phones. Some players extract whole contact lists: apps ask for consent to do this, but it is not always easy for users to consider giving their consent or what that consent in fact means.

Contact data cannot be considered in isolation as individual data about users: it is interesting because it says something about relationships. That is to say, this data says something about users and their relationships with the world around them (friends, interests, work). The people behind applications for social networking sites are particularly interested in data like this, as are marketing companies. The more concrete data is available, particularly that which app users themselves put in their phones, the more valuable it is.

¹³ Opinion 13/2011 on Geo-location services on smart mobile devices

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf

¹⁴ IMEI stands for International Mobile Equipment Identity, and is a kind of serial number for phones

¹⁵ Such as the Microsoft Media Player case from 2002

<http://www.wired.com/politics/security/news/2002/02/50567> and <http://news.cnet.com/2100-1023-955514.html>

¹⁶ Ekomforskriften [Regulations on electronic communications networks and services] § 7-3:
<http://www.lovdatab.no/for/sf/sd/td-20040216-0401-008.html#7-3>

3.1.4 Calendar data

Some applications write data to calendars or take data from them. Calendar data shows not just what people do, but also where they will be travelling in the future and where they have travelled in the past (location) and who they relate to. By synchronising with your employer's calendar, for example, what users put in their calendar may also be visible to employers, colleagues and others who can access your employer's calendar without users being aware this is happening.

3.1.5 Cameras and microphones

Cameras and sound activation are hardware operated (hardware controls). Applications that can access users' cameras can use these when app users ask for them. You may need to allow an application to access your camera to use other elements, such as lighting or flash. Some apps activate cameras without telling users they are doing so, however. The same goes for sound. The media have presented US image sharing app Color App as an example of an app that activates microphones without telling users it is doing so¹⁷. In this case it is not natural for users to assume the app will record noise either, as the purpose of the service is to share images.

3.1.6 Gyroscope and accelerometer

Gyroscopes and accelerometers are hardware controls which can tell a lot about app users. Such functions are perhaps most visible in connection with games applications: they record the movement made to carry out activities on smart phones, such as skipping to the next track in the music player. Such functions can also be used to report movements to others and third parties: they are so precise, they can say a great deal about what a given app user is doing at any given time, whether you are sitting quietly, walking along or jogging. They can also indicate whether you are eating or on a bus. Apps have also been developed which can report on users' sleep patterns by people putting their mobiles in their beds. There is work on gait biometrics (Nislab on HIG and gait biometrics) which can tell people apart by what is happening on their mobiles' motion sensors.

Gyroscopes and accelerometers will become increasingly important in future as these functions become more actively used. These functions are particularly interesting when it comes to identifying people and their activities. As with location data, these functions will be particularly important in terms of data protection.

¹⁷ http://www.computerworld.com/s/article/9215853/Snooping_It_s_not_a_crime_it_s_a_feature

4 Lack of transparency

4.1 System based on trust

Users will, when installing and using apps, to a greater or lesser extent allow those apps to access data on their mobiles. When downloading apps, users must consider whether they trust that personal data will be used acceptably. As users have only a limited ability to see what data is being collected, what is done with it and who is legally responsible, such transactions are based to a large extent on trusting the different app players involved.

iPhone users leave how their personal data is handled to Apple, which by approving all apps in advance ensures they meet certain requirements. From a user's viewpoint, we could compare how the iOS platform handles personal data with opening a *huge door* into their phone. Once this door is open, users will not know definitely what data passes through it, but have to rely on Apple having full control over apps and what they can extract, i.e. that Apple keeps an eye on who can access the data passing through the door. It is difficult for iPhone users to assess whether they can trust apps in themselves, as they are not told what information is being collected and who is legally responsible for an app. So the system is based on users trusting Apple.

Android users are left to their own devices more than their iPhone counterparts when it comes to considering whether apps will use personal data responsibly or not. Android does not accept liability for its apps meeting any given minimum requirements in this respect: before installing apps, users must consider whether they will give the app access to the data elements they list. Amongst other things, users must consider whether access given to the app meets their own security demands for the personal data that are disclosed. Android users have to decide for themselves whether the people or businesses who supply apps inspire confidence. It is not always easy to define who is responsible for an app.

The way Android handles personal data may be regarded as opening a number of *small holes*, unlike Apple, which opens *one* large door. Once these holes are open, users have little control over what goes through them, however. There is no other authority that watches over this. Users may end up installing applications that appear to open holes (open for information) they do not wish to allow the application to access. Compared with iPhone users, Android users will however be able to have a more qualified evaluation about each application before downloading it. But Android users must also base installing apps on trust. Users have to trust the various players involved not to misuse the data they are given access to on their phones.

4.2 Absence of information

The Norwegian Personal Data Act gives citizens rights in cases in which businesses process data about them. To exercise these rights, they must know that data is being processed, and they must know their rights. Being told data is being processed is particularly important in cases where it is not intuitively obvious to citizens that this is happening. Under section 19 of the Personal Data Act, customers must be informed amongst other things as to why personal information is being processed, whether it will be disclosed to third parties and so on.

By publishing a privacy policy, businesses which make applications will put users in a better position to exercise their rights under data protection legislation. A good privacy policy is something app-managers can earn from, as it creates more trust between them and their users.

Privacy policies may be included within apps or put on Android Market or App Store. One advantage of having information available on Android Market or App Store is that it is then available to users before they install the app. By installing an app, users give presumed consent to processing their personal data: so it is essential they have the information they need *before* they install apps. If this information can only be found in the app itself, that amounts to informing users *after* they have given their consent – which is the wrong way round. The *benefit* of including the information in the app too is that it can then be revoked easily if users later discover how their personal data is used. That may lead to users wanting to revoke their consent by uninstalling apps.

It would benefit users if details of how apps use personal details were also available on businesses' normal websites: that would make the information more available, and help indicate who is legally responsible for an app. Having privacy policies on websites would also indicate whether apps are covered by Norwegian legislation, particularly given that apps are downloaded from international players like Apple and Android, for example.

Of the 20 Norwegian Android apps the Data Inspectorate looked at, none have readily accessible data protection statements, on Android Market, the app owner's website or within the apps. Just how hard it is to find good, relevant information on who is legally responsible for an app and how they handle personal data can be shown by the example illustration below:

The Trafikanten¹⁸ App for Android states in connection with downloading from Android Market that the data it handles is as follows:

- Your location, detailed (GPS) location, rough (network based) location
- Network communications, full internet access
- Your personal information, for which read contact data
- System tools, change WiFi status, stop phone being deactivated
- Network communications, via network status, via WiFi status
- Hardware controller, controller vibrator

Much of this must be regarded as personal data.

When Trafikanten was installed for **Android**, some additional information was given in English. This said amongst other things that contact data would be collected to locate users' contacts, so users could be directed to stops nearest to their friends. It also said that the app can only access GPS data.

The same app, Trafikanten for Android, says this app was developed by a private individual jointly with Trafikanten. It does not say who is legally responsible for processing personal data. All fault reports and feedback must be made via this individual's gmail account.

¹⁸ The Trafikanten App is a real-time travel planner covering the capital Oslo and surrounding area.

Trafikanten's **iPhone** app says nothing as to who is legally responsible for processing personal data, but says more information is available at trafikanten.no. It also refers to copyright for Trafikanten AS and Shortcut AS (the app developer).

Nothing is said about collecting and using personal data when Trafikanten for **iPhone** is installed, nor if you go on to the developer's website it is linked to.

Trafikanten.no says a bit about the company's apps for iPhone or Android; but it does not say what personal data they gather when they are used. In its data protection statement, trafikanten.no merely says how the website itself handles personal data; there is no mention of the apps. So users will not know how their personal data is handled or by whom when they install Trafikanten apps.

The example of Trafikanten shows there are many ways of informing users: on App Store and Android Market, in the app itself, or on the app manager's website; but opportunities to inform users are rarely used.

5 Who is in charge?

Users need to know *who* is legally responsible for processing the personal data collected: unless they know this, they cannot exercise their rights under the Personal Data Act. They cannot, amongst other things, check that the data is being handled correctly, that no more data is processed than is necessary and that the data is deleted immediately if it is no longer required for processing.

There are many players in the app market, as we saw in section 3.3. Users would find it hard to ask all the players about access to their data to assure themselves it is being handled correctly.

One key challenge here is that the app market is global. App developers offer their products on global platforms, from which users can download them anywhere in the world. The enormous range of applications available, written by developers worldwide but available in global app stores, means consumers cannot be clear what country's law any given app comes under.

If an app complies with US law, it may differ considerably from Norwegian law or the European Data Protection Directive. The requirements which are considered as applying in Norway and Europe do not necessarily apply to companies under US law. In view of these differences, the EU and USA have established a special treaty governing the transfer of personal data, the Safe Harbor framework¹⁹, aimed at getting US processing managers to meet the requirements of an 'adequate level of protection' in Art. 25 (1) of the Directive, which corresponds to section 29 of the Norwegian Personal Data Act. The Safe Harbor framework applies only to transfer of personal data from EU / EFTA member states to the USA.

Apps supplied via App Store must in principle comply with US law and the terms Apple lays down; but applications initiated by Norwegian players aimed at Norwegians must also comply with Norway's

¹⁹ http://www.datatilsynet.no/templates/article_2626.aspx

Personal Data Act. How apps, including third parties, comply with Norwegian law is something that will have to be clarified by app managers for all current platforms, iOS, Android etc.

5.1 A data controller must be identified

It is important to clarify who the data controller is for each application²⁰. The controller has amongst other things a duty to inform how personal data is handled. It is important to identify who is legally responsible in each case, with reference to the purpose of collecting personal data and the contractual relations between the parties.

5.1.1 Relations between developers and clients

Application developers write apps, so it is they who know most about how their applications handle personal data. Application developers know what third parties are involved in the next link to their apps, such as analysis and statistics companies, location companies and marketers.

Many app developers are small organisations who often lack the resources and know-how required to look at data protection law or how it is handled by the platforms they upload their apps to. The platforms have a major role to play in ensuring that customers are well protected, but app developers must take responsibility for what they do themselves – they cannot rely on platforms and assume that they will be responsible for good security and data protection.

In the Norwegian app market particularly, apps are usually developed for clients: 13 of the 20 Norwegian applications the Data Inspectorate looked at in this report were developed to order. It is the client who defines what an app should be like, and it is only natural that the business concerned should then be the data controller. The challenge to the client is that it may be difficult to get a complete picture of how the application handles personal data and what third parties are involved, as they often have not themselves been involved in the programming of the app (see previous section). This means it may be challenging for clients to make good privacy policies for their users.

Clients often want to get access to the personal data that applications collect, because this tells them who the customers are and how they use the app. If the developer manages the app and handles personal data on the client's behalf, a data processing agreement is required.

It is not always the person who appears as the client who actually took the initiative to create an app. The person who appears to be the client may have been offered an app by an app developer. The developer may have been allowed to use logos and the name of a company, preferably by agreement with that company, but without necessarily taking responsibility for the app itself. There may be developers who have their own financial or other interests in creating apps under someone else's logo.

²⁰ A controller is the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data. A 'processor' is the natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

5.1.2 Dealings with third parties

Third parties can be divided into a number of groups, as we saw in section 3.3.3, such as analysis companies, marketers and location service providers who basically provide services to app developers. In principle, the controller cannot disclose personal data from apps to third parties without setting up data processing agreement under section 15 of the Personal Data Act.

Data processors usually deliver a paid service for controllers. In the app world, as we said before, it is often unusual to take payment in cash for the services provided. Personal data may also be used as a currency. That means third parties do not merely provide services to app managers as data processors, but that they also process and pass on personal data independently. If personal data is given to third parties for their own purposes, those third parties must also be identified as controllers and comply with Norwegian law.

Many of the much used third party providers act outside Norwegian and European law. Such companies often use standard contracts with other parties without informing how they use personal data for their own purposes. It is important that those involved in developing apps, both app developers and clients, take the necessary steps to take control of what third parties do with personal data further down the line.

6 Other legal issues

6.1 A contract is the foundation

Under the Personal Data Act some conditions must be met before processing of personal data can be initiated. These conditions are that processing personal data is either authorised in law or is based on the active consent of those registered. Under the Personal Data Act, those responsible for processing may only use personal data for explicitly stated purposes the law allows. Personal data must not be used subsequently for purposes which are incompatible with the purpose for which it was originally used without consent. When buying goods and services which also require some personal data to be collected and used, the foundation in law will normally be found in section 8 a) of the Personal Data Act. This says that personal data can be processed, i.e. collected and used, if this is necessary to *fulfil contracts* with customers. The reason this contract option is the most relevant to apps, as a starting point at least, is that personal data often has to be processed to perform contracts with customers. These contracts per se, on the other hand, will not be about processing personal data but about getting products or services.

Section 8 a) of the Personal Data Act states that the controller may process personal data about customers which is necessary to fulfil contracts with them. This imposes limits on how much personal data the controller can collect and use on this basis in law – one way or another, such collection and use must be necessary to fulfil the contract. If personal data is collected and used beyond what is necessary to perform the contract, this in turn must be justified in law. The most natural course of action would be to obtain the customer's consent to collecting and using personal data beyond what is needed to fulfil the contract.

One question that will probably often arise is what data, strictly speaking, is needed to perform contracts, and, not least, who is to consider whether it is necessary. To some extent, it is up to the controller to consider what their business needs to perform contracts, but it must be considered whether a business's assessment is reasonable and rational.

6.2 Rights of inspection and information

The lack of clarity about responsibilities in the app market means app users will not find it easy to exercise their right to access the personal data that different businesses process.

Both in terms of contracts and consent as the foundations for processing personal data in law, it is a prerequisite that customers must be told how their personal data will be handled. That customers should know what data is collected and used follows on from the assumptions about the basis for the processing itself – you cannot enter into a contract or consent to something if you do not know what it involves. The right to access also follows from section 18 of the Personal Data Act. It also follows from section 19 of the Personal Data Act that customers must be informed amongst other things as to what purpose their personal data is used for, whether it will be disclosed to third parties, etc.

Section 21 of the Personal Data Act may also be relevant if personal data is used to create personal profiles. If personal data is collected and processed when we buy and use apps, customers are entitled to see any and all data processed about them. This provision must be taken to mean that

anyone who buys an app has the right to find out what kinds of personal data are used, what they are used for and whether they are passed on to third parties.

Customers could contact those responsible for the Trafikanten app and demand under the law that all data processed in connection with their use of the app be given up.

Under the Personal Data Act, those legally responsible for dealing with applications which use personal data must give details of:

- Who is legally responsible for the app
- What is the purpose of the processing of personal data
- What personal data is processed
- Whether that personal data will be passed on and, if so, to whom
- About deleting personal data
- Security measures
- Anything else that enables those registered to use their rights
- What law (jurisdiction) the app is subject to in terms of processing personal data

6.3 Relations with other legislation

When individuals buy products or services, this usually is subject to legislation other than the Norwegian Personal Data Act. As for buying apps for mobile phones, such transactions under Norwegian law are governed mainly by the Act on Consumer Purchase (insofar as they are within the jurisdiction of that law). The purpose of the transaction is to obtain a product (game, weather service, etc.). The main purpose of the transaction is not that those responsible for the processing can process personal data about the customer. This is a side effect as far as the customer is concerned.

The Act on Consumer Purchase also has provisions on the lack of information on products. Under this law, products are held to be defective if the vendor neglected to disclose essential aspects about the product at the time of the sale which might have been expected to influence the decision to buy.

7 Conclusion

In conclusion, the Data Inspectorate finds:

- App users are not adequately informed about *which* data is collected about them, *what* it is collected *for*, or how the data may be *reused*.
- It appears unclear to the Data Inspectorate who is legally responsible (the controller) for applications that collect personal data.
- App users' *right to access* their personal data that has been collected is difficult to exercise when there is no indication of who is legally responsible for the processing (who is the controller).
- Existing opportunities to explain how apps use personal data on App Store or Android Market are seldom used. If this were done more often, users would be in a better position to decide whether to install apps or not before downloading them.
- Available opportunities to explain how personal data is used within apps are rarely used. It is worth including information here, too, so it is easily available to users once they have downloaded the apps. However, if information is given *only* inside the apps, users will only be informed *after* they have given their consent when downloading the apps – this is the wrong way round in accordance to the Personal Data Act.
- The opportunities to explain how apps use personal data on app managers' websites are rarely used. This is unfortunate, as a publication of privacy policies would make information more available and clarify for the user who is legally responsible for the apps. It would also clarify which legal system (jurisdiction) the apps fall under in terms of using personal data.

8 ANNEXES

Annexe 1: Norwegian Android apps studied in report.

Android apps			
Norwegian	Responsible/client	Developer	Paid / free
DNB Nor	DNB Nor (uncertain)	avantime.se	Free
Nordea	Nordea (uncertain)	nordea.no	Free
Fokus Mobilbank	Fokus Bank	(Not clear)	Free
Gulesider	Eniro	(Not clear)	Free
Matprat	Egg and food information office	SmartpPhones Telecom	Free
YR.no Widget	Øystein Gulliksen	Øystein Gulliksen	Free
Wimp	Aspiro Music	Aspiro Music	Free
Trafikanten offisiell	(Not clear)	Anders Aagard	Free
TV 2 Sporten	TV 2	(Not clear)	Free
Posten sporing	Post office	(Not clear)	Free
NRK Radio	NRK	NRK(uncertain)	Free
Gjensidige	Gjensidige	Making waves	Free
Norsk Tipping	Norsk Tipping	Agens(uncertain)	Free
TaxiNå!	Apphuset	Apphuset	Paid
7-Eleven Norge	7-Eleven Norge	Apphuset	Free
Holmenkollen Ski-Jumpt	Norsk Tipping	Norsk Tipping / Agens (uncertain)	Free
Visit Norway	Visit Norway	Making waves	Free
Norsk TV-guide	Apps for a better world	Apps for a better world	Free
Norsk Radio	Apps for a better world	Apps for a better world	Free
Flyplass Pro	Frank Burmo	Frank Burmo	Paid

Annexe 2: Foreign Android apps studied in report

Android app			
Foreign	Responsible/client	Developer	
Spotify	spotify ltd	spotify ltd	Free
Shazam	Shazam	Shazam	Free
Fruit Ninja	Halfbrick Studios	Halfbrick Studios	Paid
Chess Online	Cloudroid	Cloudroid	Free
Barcodescanner	Zxing Team	Zxing Team	Free
Evernote	Evernote corp	Evernote corp	Free
Fingerprintsscanner	ComputerTime Co	ComputerTime Co	Paid
Twitter	Twitter	Twitter	Free
WhatsApp Messenger	WhatsApp Inc	WhatsApp Inc	Free
Skype	Skype	Skype	Free
Google Maps	Google	Google	Free
Doodle Jump	Game House	Game House	Paid
SoundHound	SoundHound	SoundHound	Paid
TripAdvisor	TripAdvisor	TripAdvisor?	Free
Vignette	Neilandtheresa	Neilandtheresa	Paid
FatBooth	PiVi & CO	PiVi & CO	Free
Facebook	Facebook	Facebook	Free
Angry Birds	Rovio Mobile	Rovio Mobile	Free
Springpad	Spring Partners	Spring Partners	Free
Tiny Flashlight	Niolay Ananiev	Niolay Ananiev	Free

Annexe 3: List of questions sent to Norwegian app developers

The aim of this meeting is to find out more about how applications need access to personal data processed on phones, such as location data, data from contact lists, calendars, sounds and images, net access records, call records, downloaded files and phone IDs. The questions we would like to discuss are as follows:

- How does your business consider this issue?
- Can services be created which work well but are also data protection friendly?
- Is it possible, for example, to develop apps in which users themselves can 'scale' what data apps can access (determine the level of functionality of an app themselves – with / without access to location, with / without access to the contact list)?
- How is data collected from app users used? How much access do clients have to user data, and what kind of data can app developers get access to? Is data sold or furnished to third parties by other means?
- How come there are so few apps with a data protection policy?
- Are there any differences between platforms when it comes to how much apps need to access personal data on phones?
- Any other data protection aspects of mobile apps that come up in discussion.

Annexe 4: Typical information page on Android Market

Typical list of information which states what Android apps need access to.

The screenshot shows the Android Market page for the 'Gulesider® Offisiell app' by ENIRO. The page is displayed in a Windows Internet Explorer browser window. The app's icon is a yellow square with a black grid pattern and the text 'GULE SIDER'. It has a 5-star rating with 877 reviews and an 'INSTALLER' button. Below the app card, there is a section 'Mer fra utvikler' listing other apps from ENIRO: 'Krak' (197 reviews), 'eniro.se' (2 060 reviews), 'Rejta' (9 reviews), and 'Panorama Firm' (36 reviews). The main content area is titled 'Tillatelser' (Permissions) and lists the following permissions: 'PROGRAMMET HAR TILGANG TIL FØLGENDE:', 'DINE KONTOER' (allows account management), 'FUNGERE SOM EN KONTOGODKJENNER' (allows account authentication), 'MASKINVAREKONTROLLER' (allows camera access), 'TA BILDER OG VIDEOER' (allows photo and video capture), 'DIN POSISJON' (allows location access), 'GROV (NETTVERKSBASERT) POSISJON' (allows coarse location), 'DETALJERT (GPS) POSISJON' (allows precise location), and 'DINE MELDINGER' (allows reading of messages). The page also includes navigation tabs for 'OVERSIKT', 'BRUKEROMTALER (248)', 'HVA ER NYTT?', and 'TILLATELSER'. The browser's address bar shows the URL 'https://market.android.com/details?id=com.gulesider.android&feature=search_result'. The taskbar at the bottom shows the Start button, several open applications, and the system tray with the time 13:10.

Annexe 6: Norwegian apps with data protection statements

	Does the app come with a privacy policy?
Norske	
DNB Nor eiendom	No
Nordea	No
Fokus Mobilbank	No
Gulesider	No
Matprat	No
YR.no Widget	No
Wimp	No
Trafikanten offisiell	Some information
TV 2 Sporten	No
Posten sporing	No
NRK Radio	No
Gjensidige	No
Norsk Tipping	No
TaxiNå!	No
7-Eleven Norge	No
Holmenkollen Ski-Jump	No
Visit Norway	No
Norsk TV-guide	No
Norsk Radio	No
Flyplass Pro	No