Mobile Privacy: Is There An App For That?

On smart mobile devices, apps and data protection

Master’s Thesis
Institute for Information Law (IViR)
University of Amsterdam

Emre Yildirim

Supervisor: dr. J.V.J. van Hoboken
Second Reader: mr. F. Zuiderveen Borgesius

May 2012
Table of Contents

List of Abbreviations .......................................................... 4
Introduction .................................................................. 5
1. Smart Mobile Devices .................................................. 7
   1.1 Manufacturers ...................................................... 7
   1.2 Application Catalogs ............................................. 9
   1.3 Software Development Kits ................................. 10
   1.4 Payment Models .................................................. 11
   1.5 Analytics & Advertisement ................................... 12
   1.6 EULAs & Privacy Policies .................................... 13
   1.7 Conclusion .......................................................... 16
2. Data ........................................................................... 17
   2.1 Access .................................................................. 17
   2.2 Available Data .................................................... 20
   2.3 Methodology ......................................................... 30
   2.4 Results ................................................................ 32
   2.5 Summary .............................................................. 35
   2.6 Conclusion ............................................................ 38
3. Applicable Laws and Jurisdiction .................................. 39
   3.1 Applicability of the Data Protection Directive .... 40
   3.2 Jurisdiction and the Data Protection Directive .. 49
   3.3 Applicability of the e-Privacy Directive ............... 54
   3.4 Conclusion ............................................................ 59
4. Analysis

4.1 Data Protection Directive

4.1.1 Legitimate grounds

4.1.1.1 Consent

4.1.1.2 Contract

4.1.1.3 Legitimate Interest

4.1.2 Proportionality

4.1.3 Legitimacy and purpose limitation

4.1.4 Transparency

4.2 e-Privacy Directive

4.2.1 Prior Informed Consent

5. Conclusion

Literature list

Appendix A
# List of Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADID</td>
<td>Application Device Identifier</td>
</tr>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>CDMA</td>
<td>Code Division Multiple Access</td>
</tr>
<tr>
<td>EULA</td>
<td>End User License Agreement</td>
</tr>
<tr>
<td>HTTP</td>
<td>HyperText Transfer Protocol</td>
</tr>
<tr>
<td>HTTPS</td>
<td>HyperText Transfer Protocol Secure</td>
</tr>
<tr>
<td>LAEULA</td>
<td>Licensed Application End User License Agreement</td>
</tr>
<tr>
<td>IP(-address)</td>
<td>Internet Protocol (address)</td>
</tr>
<tr>
<td>MAC(-address)</td>
<td>Media Access Control (address)</td>
</tr>
<tr>
<td>(M)OS</td>
<td>(Mobile) Operating System</td>
</tr>
<tr>
<td>SDK</td>
<td>Software Development Kit</td>
</tr>
<tr>
<td>SMD</td>
<td>Smart Mobile Device</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
</tr>
<tr>
<td>UDID</td>
<td>Unique Device Identifier</td>
</tr>
<tr>
<td>UMTS</td>
<td>Universal Mobile Telecommunications System</td>
</tr>
</tbody>
</table>
**Introduction**

Snap a photo with your camera. Geotag its location using GPS. Apply a funky retro filter using your favorite photo editing application. Simultaneously share it with your friends by e-mail, Twitter and Facebook. The capabilities of smartphones and tablets are endless. Smart mobile devices are more popular than ever now, and are part of everyday life of their users; we bring them everywhere we go.\(^1\) Their communication and connectivity capabilities ensure that we are always connected to the outside world.

An important shared feature of smart mobile devices (‘SMDs’) is the ability to purchase, download and install applications (‘apps’) that are available in application catalogs. Application catalogs are immensely popular as they give users the ability to enhance and enrich their device according to their personal needs, by downloading apps of their interest. The majority of these apps are developed by third parties.\(^2\)

The fact that smart mobile devices are personal and intensively used, ensures that they hold a lot of data; this results in a goldmine of (personal) data that can be of interest to third parties. As smart mobile devices have become more popular and widespread, various privacy concerns have been raised. Several studies regarding apps showed that personal data was widely processed.\(^3\) Diverse (class action) lawsuits have already been filed around the world for unauthorized processing of personal data by apps. Users are concerned: according to a research published by the GSM Association, 92% of the respondents expressed their concern about apps collecting ‘personal information’ without their consent.\(^4\) During the course of writing this thesis, mobile privacy was frequently in the spotlights on several occasions: new privacy issues were reported, while at the same time various initiatives to enhance mobile user privacy were launched. It is expected that mobile privacy will receive a greater focus in the future. Several

---

1 The term smart mobile devices in this thesis refers to smartphones and tablets.
2 Apps that are developed by third parties, as opposed to apps that are developed by the manufacturer of the mobile operating system or the operator of the application catalog, are referred to as ‘third-party apps’.
bodies involved in data protection in Europe have already made mobile privacy a focus of their work program for 2012.\(^5\)

Mobile privacy has been described as *terra incognita*.\(^6\) The source of the privacy concerns is twofold; firstly because apps can access a lot of personal data available on smart mobile devices, secondly because the processing of personal data by apps is not always transparent to users.

The goal of this thesis is to research to what extent third-party apps for smart mobile devices have to comply with relevant EU legislation concerning the processing of personal data.

To be able to answer this question, first the world of smart mobile devices, catalogs and apps is explored in chapter one, to get a overview of the involved stakeholders. Second, a technical sidestep will be taken in chapter two. This will demonstrate what kind of data are available on smart mobile devices, to what extent developers of apps can access them with or without permission of users, and how these are processed by apps. Chapter three will deal with applicable laws and discusses their substantive scope and jurisdiction. Chapter four will finally form a legal analysis of the applicable laws with respect to apps. The focus in these last two chapters is set on Directives 95/46/EC and 2002/58/EC of the European Union.\(^7\) Where relevant, the results from chapter two will be evaluated from a legal point of view, in chapters three and four.

Due to the scope of the thesis, two topics will only be discussed briefly. These topics are behavioral advertising in general and the specific roles of analytics and advertising companies as data processors and/or data controllers, and the discussion about whether article 5 section 3 of Directive 2002/58/EC enforces an opt-in or opt-out regime.

---


1. Smart Mobile Devices

Smartphones and tablet computers are like Swiss Army knives. They combine various functions into a single device: they are digital cameras, portable media players, GPS navigation units, gaming consoles and are connected to the internet via Wi-Fi or Wireless Wide Area Network (e.g. UMTS, CDMA). Smart mobile devices are popular. The adaptation of smart mobile devices is rising. Research by Nielsen shows that by January 2012, the penetration of smartphones was 50.4% in the United States.8 In the Netherlands the penetration has reached 51% according to research by Telecompaper, and it is expected that this figure will continue to grow.9

In this chapter a brief overview will be given of smart mobile devices to get a better understanding of their operation and the involved stakeholders. This will include devices and mobile operating systems, along with the functioning of application catalogs and their relationship with Software Development Kits. Furthermore payment models and their connection with analytics and advertising companies will be discussed. Finally a closer look will be taken at the triangular relationship between users, publishers of apps and operators of application catalogs, by examining how End User License Agreements and privacy policies are implemented in catalogs and apps.10

1.1 Manufacturers

Although the smart mobile devices market consists of multiple players, it is currently being dominated by Apple and Google.11 Other players on the market are, inter alia, Research in Motion with its Blackberry devices and Microsoft with its Windows Phone 7 mobile operating system.

---

10 The phrase ‘user’ in this thesis can - depending on the context in which it is used - refer to either a user of a smart mobile device and/or application, a data subject in the sense of the Data Protection Directive, or user in the sense of the e-Privacy Directive.
The current line-up of Apple’s SMDs consists of the iPhone smartphone, the iPad tablet and its iPod touch portable media player.\textsuperscript{12} All of these SMDs run on the same mobile operating system (‘iOS’) developed by Apple, and share similar features.\textsuperscript{13} The fifth and latest version of its iOS mobile operating system, dubbed iOS 5, was introduced by Apple on 12 October 2011.

A unique selling point of Apple’s iOS devices (‘iDevice’) is the system created around it. iOS is closely integrated with Apple’s iTunes software, that includes the iTunes Store. The iTunes Store and App Store, also available on iDevices as apps, lets users download music, movies, television shows, books and apps to their iDevices. The iTunes software can furthermore be used by users to manage their device (e.g. data syncing), or to update their device to the latest available iOS version.\textsuperscript{14} Updates to iOS are pushed to all devices, which makes it a uniform experience for their users.\textsuperscript{15} Whether users are on their iPhone or iPad, they have a similar experience across all devices that is complemented by the fact that they can sync their apps across multiple iDevices.

According to the latest figures announced by Apple on 4 October 2011, over 315 million iDevices (iPhones, iPads and iPod touches) have been sold worldwide.\textsuperscript{16}

Although Google did release three smartphones to date in cooperation with other manufacturers, its core business is not manufacturing SMDs. Instead, Google develops a mobile operating system for use by other manufacturers: Android OS.\textsuperscript{17} The open source nature of Android makes it possible for manufacturers to adapt Android for use on their SMDs.\textsuperscript{18} Among

\begin{flushleft}
\textsuperscript{13} Although they run on the same mobile operating system, each device gets a specific version due to differences in connectivity between the devices. The iPod touch and iPad for example lack phone functionality.
\textsuperscript{14} With the introduction of iOS 5, Apple is also providing over-the-air updates to their iOS devices. Users are therefore not any longer tied to the iTunes desktop software to update their devices.
\textsuperscript{15} Older generation devices however are eventually cut off by Apple from any further updates.
\textsuperscript{17} The Nexus One was Google’s first flagship smartphone build in cooperation with the Taiwanese manufacturer HTC, while the Nexus S and Galaxy Nexus were build in cooperation with the Korean manufacturer Samsung. Google typically introduces a new flagship smartphone with major releases of its Android OS.
\textsuperscript{18} The Android OS source code is available under the GNU General Public License version 2 and the Apache License version 2. See <http://source.android.com/source/licenses.html>.
\end{flushleft}
the manufacturers who use the Android OS for their SMDs are HTC, LG, Motorola, Samsung and Sony Ericsson.\textsuperscript{19} 

The Android OS is integrated with Google’s services, and offers similar features as Apple’s iOS. Users can purchase apps and music in Google Play - formerly known as the Android Market.\textsuperscript{20} Unlike Apple’s iOS however, updates to Android devices are generally not centrally distributed. They are instead made available at the discretion of the manufacturer of an Android device. This leads to fragmentation of the platform, because users can not always update to the latest available version of Android OS.\textsuperscript{21} 

According to the latest official figures announced by Google, more than 300 million Android devices have been activated.\textsuperscript{22}

\section*{1.2 Application Catalogs}

Smart mobile devices utilize an application catalog where users can browse, purchase and download apps on their devices. The application catalog offered by Apple is called the App Store, and Google’s the Android Market.\textsuperscript{23} 

The App Store and Android Market are accessible as an on-device app. On personal computers they are respectively available within the iTunes software, or the Android Market website.\textsuperscript{24} The ability of users to customize their device with apps that are of their interest, created a huge boost in the popularity of application catalogs and apps. When Apple’s App Store was initiated in 2008, there were merely 500 third-party apps available. Today the App Store has more than 585.000 apps available, with over 25 billion downloads to date and a continued one

\textsuperscript{19} A list of all Android OS SMD manufacturers is available at: <https://en.wikipedia.org/wiki/List_of_Android_devices>.  
\textsuperscript{20} In March Google rebranded its services for downloading media, including the Android Market, to Google Play. In the course of this thesis - for the sake of clarity - Google Play, and in particular Google Play’s Android Apps, will still be referred to as the Android Market. See Google, ‘Introducing Google Play: All your entertainment, anywhere you go’, 6 March 2012, available at <http://googlemobile.blogspot.com/2012/03/introducing-google-play-all-your.html>.  
\textsuperscript{23} Other examples of catalogs are Blackberry App World by Research in Motion, Windows Phone Marketplace by Windows, Ovi Store by Nokia, Palm App Catalog by Palm. Third party catalogs are also available for the Android OS, an example of this is the Amazon Appstore.  
billion downloads per month. The Android Market has more than 500,000 apps available, with over one billion downloads per month.

Apple’s 2009 iPhone commercial called “There’s an App For That” comes pretty close to reality regarding the variety of apps. You can find apps that will help you cook the perfect soft boiled egg or record what you are talking about during your sleep. The possibilities are almost endless. Apps range from social networking to health, and comprises of 21 different categories.

The large amount of available apps can be explained by the ability of third-party publishers and developers to create apps (‘third-party apps’) with a Software Development Kit. The popularity of apps and the anticipation of great profits have lured many publishers to create apps.

### 1.3 Software Development Kits

Native apps for iOS and Android are respectively developed with the iOS and Android SDK. Both SDKs are freely available, although publishing developed apps in the application catalogs requires registration.

A SDK combined with an Integrated Development Environment (‘IDE’) allows developers to program and design every aspect of their app: from the design of the graphical user interface, to the incorporation of available data on the SMD. It also allows them to closely integrate specific features of a SMD - such as the camera, microphone or GPS - in to their apps. Finally, they can also request data from the device, such as the address book, technical details or calendars.

---


28 The phrases ‘developer’ is interchangeable with ‘publisher’ throughout this thesis. The phrase developer is preferred over publisher when discussing technical aspects of apps.

29 In this thesis the phrase ‘developers’ is used in the context of technical implementations of an app. Where legal obligations and rights are concerned, the phrase ‘publisher’ is used.

30 Contrary to web applications that run in the web browser, native applications are installed and run directly in the mobile operating system. This allows them to integrate and interact with the mobile operating system and they thus have far greater possibilities in comparison with web applications.

31 The App Store and Android Market require developers to sign up for respectively the ‘iOS Developer Program’ and a ‘Developer profile’ in order to be able to publish applications. See <https://developer.apple.com/programs/ios/> and <https://market.android.com/publish/signup>.
Developers however do not have access to all data on SMDs. Due to the sensitive nature of some data, access can be denied, restricted or require prior permission from users. Data that is available on SMDs and retrievable by SDKs, will be discussed in depth in chapter two.

1.4 Payment Models

Four models of payment can be found in application catalogs: the (1) free, (2) free and in-app purchase, (3) paid and (4) subscription.\textsuperscript{32}

The free payment model (1) is self-evident. There can be multiple reasons for publishers to choose this model. A publisher can generate revenue from in-app advertisement, make the app popular to follow up with a paid version, introduce a light version of the paid app with limited functions or simply be generous.

Similar to the free payment model is the free and in-app purchase model (2), that is also known as the ‘freemium’ model. The difference with the former is that users can purchase ‘upgrades’ from within the app. Upgrades can consist, \textit{inter alia}, of an upgrade to a full version of the app, removing in-app advertisement or purchasing downloadable content.

The paid payment model (3) is self-explanatory. Publishers can choose the pricing of their apps as they wish.

The subscription model (4) lets users subscribe to apps for a certain length of time for a price that is set by the publisher. Like the freemium model, these purchases can be made from within the app.

Application catalogs typically share a certain percentage of revenue between the publisher of an app and the provider of the catalog, or other involved parties. In case of the App Store and the Android Market, publishers of apps receive 70% of the revenue that their app generates. The fact that application catalogs are a lucrative business for publishers can be demonstrated by the amount of money that is in the business: Apple alone has already paid out US$ three billion to publishers.\textsuperscript{33}

There is a clear relationship between apps that adopt the free and freemium payment models and mobile advertising companies, because it is an easy way for publishers to monetize

\textsuperscript{32} The availability of a certain payment model depends on the application catalog.

\textsuperscript{33} Apple Special Event, 4 October 2011, available at: \url{http://www.apple.com/apple-events/october-2011/}. 
their apps. A study of apps in the Android Market \((n = 250.000)\), showed that \(73\%\) of the apps were free.\(^{34}\) A sample of 50 apps from those free apps showed that \(77\%\) was supported by advertising.\(^{35}\) Free apps generally generate more users, which leads to higher profits of publishers through advertising. The trade-off for users is that they can download apps without cost, in return for in-app advertisements and possibly the collection of data by advertising companies. Some apps also offer the option to remove advertisement by an in-app purchase, or to install the paid version of the app which does not feature advertisement.

### 1.5 Analytics & Advertisement

Analytics and advertising companies are surging on SMDs. Imagine an advertisement campaign aimed at adult males that are between the ages of 25 and 30, who have a love for cooking and reside in Rome. Mobile advertising companies can make that happen with behavioral targeting.

All the data they need are available on, or can be retrieved with, SMDs. Personal details can be retrieved from user profiles required by an app (if they are subsequently shared with the advertisement company, which is a possibility that various advertisement SDKs offer), while the location of users can be precisely or coarsely retrieved using GPS, or Wi-Fi and GSM triangulation.\(^{36}\) The interests of users can be inferred by tracking the kinds of apps that they have installed on their SMDs, with the help of unique identifiers.

Advertising companies often make their own SDKs available, that developers can easily integrate in to their apps. One line of code incorporated in an app can be enough to display in-app advertisements. Publishers typically get paid by traditional web advertisement compensation methods like cost-per-click and effective-cost-per-mille, alongside new methods like pay-per-install (of an app).

No matter what payment model a publisher adopts, analytics are key to understanding customer behavior. Mobile analytics companies allow publishers to track what their users are doing, with an easily integrated SDK. The analytics SDK takes care of tracking users, also across

---

\(^{34}\) Leontiadis et. al. 2012, p. 2.

\(^{35}\) Idem.

\(^{36}\) Advertisement company Mobclix for example offers developers that use their SDK the option to share information about a users ethnicity and religion alongside marital status and education. The SDK is available at: [https://developer.mobclix.com/auth/register](https://developer.mobclix.com/auth/register) (sign-up required).
apps, with the use of unique identifiers. The tracking of users could also be used to build profiles of users. The level of tracking is detailed: the amount of users (total, new, active) by country, sessions and frequency of app usage, specific events (e.g. user took a photo, user pressed invite button) and the popularity of device models and carriers.

Advertising and analytics companies run on (personal) data. Most advertisement and analytics SDKs have a standard set of data that is collected, which is not alterable by a developer. The SDKs often provide optional methods for developers to send more information about users. Some analytics and advertising companies oblige publishers to inform users about their use of analytics and advertisement services. There are several identifiers available that analytics and advertising companies use to track users. These will be discussed in depth in the following chapter.

1.6 EULAs & Privacy Policies
With the use of application catalogs, several legal questions come to mind regarding the legal relationship between users, operators of application catalogs and publishers of third-party apps (‘publishers’). Are operators of application catalogs responsible for third-party apps? Are publishers obliged to provide an End User License Agreement (‘EULA’) or a privacy policy if they process personal data? A clear overview of the legal relationships between them can help understanding the duties and the responsibilities they carry.

Android Market
The Android Market Terms of Service governs the use of the Android Market, and forms a legal agreement between Google and a user. Regarding liability, Google explicitly exonerates itself from liability for apps in the Android Market that do not originate from Google. As such, Google deems itself not responsible for third-party apps that are available in the Android Market.

---

37 The inspection of various SDKs of analytics and advertising companies shows that developers can not change what data is collected by default. The provided SDKs are pre-set, and sometimes closed sourced in the form of static libraries. Customization is only available to the developer to supply more information about a user, or to incorporate the visual aspects of advertisements. See the Getting Started guide to the SDK of Flurry analytics for an example of this practice: <http://support.flurry.com/index.php?title=Analytics/GettingStarted>.


39 Article 1.2 Android Market Terms of Service.
The nature of the relationship between publishers and users is not explicitly stipulated in the Android Market Terms of Service. However, the Android Market Developer Distribution Agreement does force publishers to give users a standard non-exclusive, worldwide and perpetual license to use their app.\(^{40}\) This license to use however does not cover any other topics.

Although publishers are not obliged by Google to provide their own EULA, they can do so to substitute the above mentioned standard license. This EULA can be used to stipulate the publisher’s and user’s obligations and rights. Google does recommend publishers to include an EULA within their app, but does not provide a designated area in the Android Market to do so.\(^{41}\) The only way publishers can provide their users with an EULA, is by providing a link in their app description, or by making the EULA available within their app.\(^{42}\) There is no mechanism in place that allows users to accept or decline EULAs before installing an app on their device.

Regarding privacy, Google obliges publishers to protect the privacy of their users.\(^{43}\) If an app processes personal data, and it is governed by the standard license of use, users have to be notified of the processing, and a ‘legally adequate’ privacy notice has to be provided by the publisher. If an app provides an individual EULA that covers the processing of personal data, the processing is governed by that EULA.

**App Store**

The App Store Terms and Conditions governs the use of the App Store, and forms a legal agreement between Apple’s subsidiary iTunes s.a.r.l and users.\(^{44}\) The App Store, according to its terms and conditions, sells ‘licenses’ to use apps. The Licensed Application End User License

---


\(^{42}\) For an example of this use, see games by Electronic Arts <https://play.google.com/store/apps/details?id=com.eamobile.tetris_eu&feature=more_from_developer#?t=W251bGwsMSwxLDEwMiwiY29tLmVhbW9iaWxlLnRldHJpc19ldS1j&hl=en_GB>.

\(^{43}\) Article 4.3 Android Market Developer Distribution Agreement.

\(^{44}\) App Store Terms and Conditions, available at <https://www.apple.com/legal/itunes/uk/terms.html#APPS>. The App Store Terms and Conditions for the United Kingdom are used for demonstration purposes. iTunes s.a.r.l. (Luxembourg) is a subsidiary of Apple and is the data controller for European users of iTunes.
Agreement (‘LAEULA’) is a standard EULA, provided by iTunes for publishers that do not implement their own EULA. It forms a legal agreement between users and publishers of apps, with Apple as a third-party beneficiary. The LAEULA is part of the App Store Terms and Conditions, and is as such assumed to be accepted by users for all apps that are covered by the LAEULA. Apple, similar to Google, claims not to be responsible for third-party apps.

Although not obliged by Apple, publishers can provide their own EULA. Apple does require EULAs of publishers to be consistent with the LAEULA, and meet certain minimum requirements. Unlike the Android Market, the App Store does provide a designated area for publishers to publish their EULA. However, similar to the Android Market, it does not provide a method for where users can accept or decline an EULA prior to installing an app. Apple recommends publishers that want users to explicitly accept their EULA, to do so within their app.

The LAEULA, that presumably covers most apps in the App Stores, gives publishers the right to process ‘technical data and related information’ as long as it is in a form that does not identify an individual. What this technical data exactly consists of is unclear. However, if and when a publisher processes personal data, there are certain obligations stipulated in the App Store Review Guidelines regarding privacy.

Every app that is submitted to the App Store gets reviewed by Apple, prior to publication. The App Store Review Guidelines (‘Guidelines’) contains rules on, inter alia, security, content and privacy. These rules are enforced by Apple during the review process. Apps that do not comply with the Guidelines can and will be rejected by Apple, according to the Guidelines.

Fig 1.1 An EULA displayed in the App Store.

---

45 Idem.
46 Idem.
48 Idem, p. 172.
49 Licensed Application End User License Agreement, section b.
The Guidelines states that apps “cannot transmit data about a user without obtaining the user's prior permission and providing the user with access to information about how and where the data will be used”. How publishers are supposed to obtain prior permission or provide their users with information, is not specified in the Guidelines.

1.7 Conclusion

Smart mobile devices are popular. Their vast array of features make them a virtually indispensable device for users. The possibility for users to enhance their devices to their personal tastes with application catalogs, caused a surge in third-party apps. On Apple’s App Store and Google’s Android Market alone, there are more than a million apps available with over two billion downloads per month. Third-party apps are developed with Software Development Kits and are integrated in the mobile operating system. They can access internal functions of SMDs such as GPS and cameras, alongside on-device (personal) data, to the extent that SDKs allow them. Apps are distributed in application catalogs with different payment models, and frequently use the services of analytics and advertising companies. A clear relationship can be seen between apps that use the free or freemium payment models and advertising companies. The legal relationship between users and publishers of apps is direct, as the application catalog provider merely acts as a middleman that sells standard licenses to use. Publishers can, but are not obliged to, adopt an EULA in lieu of the standard license to use. Although catalog providers claim not to be responsible for third-party apps, they do deem it necessary to oblige publishers to implement privacy policies if personal data is processed.

---

50 Article 17.1, App Store Review Guidelines.
2. Data

In December 2010, *The Wall Street Journal* published an article about apps in its investigative series on data privacy.\(^{51}\) The study analyzed the data that 101 iOS and Android apps collect and share. The results demonstrated that apps collect and share location data, unique device identifiers, personal details and more, often without informing their users.

This chapter will take a look at what kind of data are accessible, retrievable and actively or passively processed by apps. An attempt to enumerate the available data will be made by taking a look at SDKs, and the possibilities or restrictions they offer to developers. Subsequently concrete examples of collected data, that have been acquired by monitoring the network traffic of apps, are demonstrated.\(^{52}\) While this chapter will not evaluate the privacy policies of the researched apps from a legal point of view, some general remarks will be made about their privacy policies. To limit the scope of the technical research, the focus is solely on Apple’s iOS mobile operating system. Important features of other mobile operating systems will be discussed as well.\(^{53}\)

2.1 Access

Developers that use a SDK have the possibility to use the ingenuity of SMDs, and gain access to all kinds of data that is stored on, or can be retrieved by them. Apps for iOS are developed with the use of the official iOS SDK. If for example a developer wants to use location data that is retrieved with the GPS function of an iPhone, it would have to do so with the help of the iOS SDK. The possibilities are not endless though.

Apple does not provide methods to gain access to *all* data that is available on an iOS device, and uses three solutions to achieve this: *sandboxing*, an ex-ante review of apps and a restrictive Application Programming Interface (‘API’).

---

\(^{51}\) Supra note 3.

\(^{52}\) Capturing and inspecting network traffic enables eavesdropping on data processed by applications which otherwise is hidden from the user. The process includes analyzing the Internet Protocol (‘IP’) packets that are used for communication to external servers by an application.

\(^{53}\) First, the goal of this chapter is not to give a complete overview of all available mobile operating systems. Second, it is likely that the data and conclusions would overall be similar in case other mobile operating systems were researched. Finally, I do not own any other SMDs besides the iPhone 4S. As a long time user I am familiar with its environment, capabilities and SDK.
Sandboxing is a security mechanism that forces apps to run individually in a controlled environment or container. Apple describes it as “every application is an island”\(^{54}\). The effect of sandboxing is that apps can be prohibited to access files that they are not entitled to by default. A concrete example of the restrictiveness of sandboxing is for example that an app does not have read and/or write permissions outside of its own container. It can not access call logs or browser history, unless Apple provides a public API to do so. Apps that attempt to read or write data outside of their container are subject to rejection for the App Store.\(^{55}\)

The ex-ante review of apps provides a mechanism for Apple to enforce rules on developers. The App Store Review Guidelines (‘Guidelines’), according to its recitals, is a living document. This is strongly manifested by the following quote in the introduction of the Guidelines:

> “We will reject Apps for any content or behavior that we believe is over the line. What line, you ask? Well, as a Supreme Court Justice once said, "I'll know it when I see it". And we think that you will also know it when you cross it.”\(^{56}\)

While there are concrete rules in the Guidelines regarding the use of for example location data, more general rules can be found as well. The Guidelines states that apps that attempt to cheat the system by stealing user data, will be removed from the App Store, while the developers are expelled from the iOS Developer Program.

Apps are furthermore limited to the use of public APIs provided by the iOS SDK. Private APIs are, inter alia, used by Apple in the standard apps that are available on every iOS device. They are for example used to manage and handle phone calls or e-mails, and thus give access to the file system on a deep level. If a third-party app attempts to use private APIs, it is subject to rejection from the App Store.\(^{57}\) With public APIs Apple is able to control how and when

---


\(^{55}\) Article 2.6 App Store Review Guidelines.


\(^{57}\) Article 2.5 App Store Review Guidelines.
developers have access to data, alongside the option whether prior permission is needed from users. The iOS SDK can be characterized as fairly liberal: at the moment only the access to location data, and accessing photos without user interaction, requires prior permission from users. This is achieved via a pop-up that is automatically presented to users by iOS. Access to the address book or calendars do not require any prior permission, and users are not notified by iOS. Notifying users about the use of address books and calendars, is therefore at the discretion of publishers.

Unlike Apple’s iOS, Google’s Android operating system uses a permission model. This is partly the outcome of the fact that Google relies on ex-post review of apps, as opposed to Apple. In order for developers to use certain features of SMDs or access data (e.g. read address book, calendar or SMS messages) in apps, they need to request permission at all times. A list of permissions is displayed to users upon the installation of an app. This list includes a short explanation by Google about what the required permissions are (e.g. ‘Network communication - full internet access’). Developers however do not need to - and can not - specify the purposes of the requested permissions, which are therefore absent in the permission list. Users have the option to allow or decline the needed permissions. In the latter case, the app can not be used. A pitfall of Google’s permission model is that a lot more data can be accessed in Android, in contrast to iOS. This includes SMS messages, browser history, or the ability to read low-level system logs of the device.

---


2.2 Available Data

The available types of data on iOS can roughly be divided in four categories:

1. Technical data
2. On-device data
3. User entered data
4. Cookies

A further distinction can be made in the categories, by whether the data is actively or passively processed. While actively processed data requires some form of user interaction, such as giving permission or entering data, passively processed data requires no user interaction at all. In chapter three an evaluation will be made of whether the available data that is discussed below, constitute personal data under the Data Protection Directive.

Technical data

Carrier data

Apple provides developers with an API to retrieve the carrier name, carrier country code, mobile country code, and the mobile network code of the cellular provider of users. The mobile country code and mobile network codes are defined by the International Telecom Union and can be used to identify cellular providers. An example of the output for a cellular provider is respectively: vfnl (Vodafone Netherlands - VEY), NL, 204, 04.

Connection type

It is possible to retrieve the current connection type of users. This can either be Wi-Fi or WWAN.

---

Device model and type, OS version and type

With the UIDevice API it is possible for developers to retrieve device types, such as ‘iPhone’ or ‘iPad’. An extension to the public API has been made by developers that allows the retrieval of the specific model of a device (e.g. iPhone 4S). It is furthermore possible to retrieve the iOS version (e.g. 5.0) and type (e.g. iOS) of the mobile operating system.

Device name

Every iOS device (‘iDevice’) has a name, which can be set by its user. During the initial setup of the iDevice without iTunes, the device name is automatically set to the type of the device (e.g. ‘iPad’). During the initial setup of an iDevice with iTunes though, the name of the iDevice - by default - is set to the first and last name that is associated with the Apple ID that is used for the iDevice. This results in the following name for the iDevice: [first_name last_name’s [device type]]. It is up to the user to change the name of its device.

![Set Up Your iPhone](image)

**Fig. 2.1 Default name of a new device set in iTunes**

In its UIDevice API, Apple provides developers to retrieve the name of the device. The description in the API mentions that the device name is an “*arbitrary alphanumeric string that is associated with the device as an identifier*”.

---

64 See UIDevice extension developed by Erica Sadun, available at [https://github.com/erica/uidevice-extension](https://github.com/erica/uidevice-extension).
IP-address

Every device that is connected to the internet has an assigned Internet Protocol address.65 Although there is no method provided in the iOS SDK to retrieve the current IP-address of an iDevice, it is still possible without using the restricted private APIs or deducing it from a HTTP-request. Apple’s iOS is based on the Darwin operating system, which subsequently is based on UNIX.66 The fact that the foundation of iOS is built on UNIX, makes it possible to retrieve networking information without using private APIs.67

Locale and country code

The locale of an iDevice forms the user’s preferences regarding language, and the region format that is in use for dates and time. It can be retrieved by developers using the NSLocale API.68 An example would be ‘nl_NL’ for a user that uses the Dutch language on its device. A country code can be distilled from the locale as well.

MAC-address

The Media Access Control address (‘MAC-address’) is a unique identifier assigned to networking interfaces. The Wi-Fi and Bluetooth modules found in iOS devices are such networking interfaces. Although Apple does not provide a public API to retrieve MAC-addresses, similar to the retrieval of the IP-address mentioned above, it can be retrieved without the use of public or private APIs.69 The fact that the MAC-addresses are unique and can not be changed, makes it an alternative to the UDID for developers, as will be explained further on.

Fig. 2.2 The ‘What is my MAC-address?’ app.

65 For more information about IP-addresses see <https://en.wikipedia.org/wiki/IP_address>.
67 Supra note 64.
69 Supra note 64.
**Timezone**

The time zone of an iDevice can be retrieved by using the NSTimeZone API.\textsuperscript{70} This will return the time zone that is currently in use by the iDevice (e.g. ‘Europe/Amsterdam’).

**UDID**

A Unique Device Identifier (‘UDID’) is an alphanumeric string that is assigned to every iDevice. It is calculated using a formula that is based on the serial number, International Mobile Equipment Identity or Electronic Chip ID, Wi-Fi MAC-address and Bluetooth MAC-address of an iOS device.\textsuperscript{71} The UDID is unique to every iDevice and is not alterable by users. The UDID was initially provided by Apple as an aid for developers to identify their users. The normal use of the UDID, as intended by Apple, was for example to store high scores of games on external servers. According to the Wall Street Journal, Apple internally treats UDIDs as ‘personally identifiable information’. When the UDID is combined with data from the Apple IDs of users, it can be used to identify an individual.\textsuperscript{72} Due to the sensitive nature of UDIDs, Apple advises developers to not publicly associate a UDID with user accounts, due to user security and privacy.

The very nature of the UDID, and the fact that it is easily accessible, makes it a perfect tool for developers, analytics and advertising companies to track user behavior.\textsuperscript{73} Users generally are not made aware of, and can not block, its use by apps. The UDID can be - and is - used by analytics and advertising companies to aggregate data, and create profiles of users based on the apps they use.\textsuperscript{74} It is therefore no surprise that most analytics and advertising companies collect UDIDs. They often provide developers with their own SDKs that can be easily integrated in to apps. As a result, apps automatically transmit data, with limited options for developers to decide what data is collected. Developers in return receive free analytics services, or have a new channel of revenue by advertisements displayed in their app.

\textsuperscript{71} See <http://iphonedevwiki.net/index.php/Lockdownd>.
\textsuperscript{72} Supra note 3.
\textsuperscript{74} Seriot 2010, p. 25, available at <http://seriot.ch/resources/talks_papers/iPhonePrivacy.pdf>.
The UDID of an iDevice can be retrieved using the UIDevice API of the iOS SDK. With the introduction of iOS 5.0 however, Apple deprecated the UDID. Although the UDID is still retrievable, the depreciation denotes that it will soon be limited for use by developers, and that developers will have to find alternatives to the UDID. The UDID is therefore in a transitional phase until further notice by Apple. Apple recommends developers to create an app specific Universally Unique Identifier (‘UUID’).

In 2010 Seriot recommended two solutions to tackle the privacy issues of UDIDs: firstly the introduction of an application device identifier (‘ADID’), and secondly the requirement of prior permission from users. The ADID would still allow developers to use a unique identifier, be it for their app only. Effectively, this would block the aggregation of data and profiling of users across apps by analytics and advertising companies, unless they create their own global UDIDs. The UDID would furthermore only be accessible by apps, and thus also analytics and advertising companies, if users gave their prior permission. It seems like Apple has chosen for the ADID.

Why Apple has chosen to deprecate the UDID remains a mystery. A good guess is that the depreciation is the result of privacy concerns. Nevertheless, the industry is already catching with what seems a cat-and-mouse game. Several ideas have been opted and are already in use by analytics and advertising companies to keep tracking users. These ideas generally use unique identifiers that are similar to the UDID. W3i, an app monetization network, suggests developers to use unique identifiers based on the MAC-address. As described above, the nature of a MAC-address is very similar to the UDID, and is thus a good candidate for an alternative to the UDID. Although the use of the MAC-address as a unique identifier is against the ratio of the depreciation of the UDID, it is yet to be seen how Apple will react to apps that are using the MAC-address as

78 Seriot 2010, p. 25.
a unique identifier. Currently there are apps available in the App Store that retrieve the MAC-address, albeit not with the specific use of a unique identifier.\textsuperscript{80}

**On-device Data**

*Address book*

The address book of users is accessible by developers with the use of a public API provided by Apple.\textsuperscript{81} Developers can access and modify all contact details without limitations, and without informing or obtaining prior permission from users.\textsuperscript{82} The address book is for example used by apps that are an alternative to the standard contacts app of Apple. The address book is furthermore used by (social) apps for a ‘find my friends’ feature.

*Calendar*

The calendar of users is accessible by developers with the Event Kit API.\textsuperscript{83} Like the address book, developers can access and modify the calendar of users, without informing or obtaining prior permission from users.

*Game Center ID*

Game Center is a social gaming platform that is developed by Apple. It is a framework for developers that allows the interaction of their apps with Game Center. Developers can store high scores of users on leader boards, or present challenges to users in order to unlock achievements. Users have to register for a Game Center account using their Apple ID. While setting up their account, users have to accept the Game Center Terms and Conditions, that are presented during registration. Users are furthermore required to choose a Game Center ID, that will be publicly displayed to other users.

\textsuperscript{80} What is my MAC-address?, published on 17 August 2010, available at \texttt{<http://itunes.apple.com/gb/app/mac-address/id386545612?mt=8>}.  
\textsuperscript{81} See Address Book Framework Reference iOS, available at \texttt{<https://developer.apple.com/library/ios/documentation/AddressBook/Reference/AddressBook_iPhoneOS_Framework/_index.html>}.  
\textsuperscript{82} Seriot 2010, p. 11.  

25
It is possible for developers to retrieve the Game Center ID of users by using the GameKit framework provided by Apple.\textsuperscript{84} Although the Game Center Terms and Conditions mention several uses of the nickname by Apple, it does not include the fact that developers are able to retrieve nicknames of users.\textsuperscript{85} While there are no requirements for users to use their real names as their Game Center ID, they can do so.

It seems that Apple has realized that the Game Center ID could be problematic and has therefore taken the following measures that are mentioned in the App Store Review Guidelines in order to prevent abuse. Section 6 of the Guidelines states that developers are not allowed to display Game Center IDs to users or third parties, and may not use Game Center IDs for any other purposes than those that are approved by the Game Center Terms and Conditions. Furthermore, developers that “\textit{attempt to reverse lookup, trace, relate, associate, mine, harvest, or otherwise exploit Player IDs, alias, or other information obtained through the Game Center will be removed from the iOS Developer Program}”\textsuperscript{86}

\textit{Location data}

Developers can retrieve the realtime location of users by using the build-in GPS of an iDevice.\textsuperscript{87} In order for location data to be retrievable though, location services need to be enabled in the general settings of the iDevice by users (see figure 2.3 left). Only when location services are enabled, can apps retrieve location data from the device.

The CLLocationManager class assists developers in retrieving location data.\textsuperscript{88} On the first attempt of an app to retrieve location data from an iDevice, iOS prompts the user with a standard pop-up that requests permission for the use of location data by that app. This prompt is illustrated in figure 2.3 (right). Although not obliged or required, developers can add a `purpose message` that will be displayed in the permission pop-up. This allows developers to inform users

\textsuperscript{86} Article 6.3 App Store Review Guidelines.
\textsuperscript{87} iDevices that do not have built-in GPS available (e.g. iPod touch, iPads without 3G/4G connectivity, use Wi-Fi based location data.
\textsuperscript{88} CLLocationManager Class Reference, available at: <https://developer.apple.com/library/ios/#documentation/CoreLocation/Reference/CLLocationManager_Class/CLLocationManager/CLLocationManager.html>.
about the purpose of the location data (see figure 2.4 left). The iOS SDK furthermore gives developers granular control over the accuracy of the retrieved location data, as they can choose to retrieve exact or approximate location data.89

In its App Store Review Guidelines, Apple requires apps to “notify and obtain user consent before collecting, transmitting, or using location data”.90 Although the above mentioned purpose message seems like the foremost place to notify users, the implementation of a purpose message is not obliged by Apple. The Guidelines finally state that apps may only use location services if they are “directly relevant to the features and services provided by the app to the user or to support approved advertising uses”.91

![Location Services settings](image1)

**Fig. 2.3 Left:** Location Services settings where users can enable and disable location services altogether or alter specific permissions for apps. **Right:** The Foursquare app with the standard prompt for use of location services by apps.

---


90 Article 4.1 App Store Review Guidelines.

91 Article 4.4 App Store Review Guidelines.
Photos

Developers are able to interact with the camera of iDevices, and have access to stored photos of users. iOS offers developers two ways of accessing photos: using a standard Image Picker developed by Apple, or alternatively with a framework that allows developers to customize how images are picked.92

The Image Picker has a standard interface, is limited to select one photo at a time and requires user interaction to select photos. The ALAssetsLibrary framework however, allows customizing the Image Picker interface, multiple photo selection and - if present - access to location data embedded in the photo.

![Fig. 2.4 Left: Dropbox app using the ALAssetsLibrary and a location permission pop-up.](image_url)

![Center: the Image Picker. Right: A customized Image Picker with the ALAssetsLibrary.](image_url)

Developers can also access photos programmatically with the use of the ALAssetsLibrary framework; malicious use of this could result in retrieving all photos of users. In order to use the ALAssetsLibrary however, Apple requires developers to obtain prior permission of users for the use of location services. This is even the case if developers do not require the use of location services.

---


28
services for their app. The ratio behind the required permission seems to be based on the fact that photos could have - and in case location services for the camera app are enabled by users do have - location data embedded. The prior permission of users is therefore not required for the use of the image library per se, but for the embedded location data in photos. This leads to a curious result: any app that obtains permission from their users to use location services, automatically has access to all their photos with the ALAssetsLibrary framework.

**User-entered Data**

The amount of data that developers can collect is endless as long as users are willing to disclose them. Especially when user profiles are made in apps, a lot of data is processed. A list of frequently collected data includes the date of birth, e-mail address, first and last name, gender, profile picture, phone number, social media account (e.g. Twitter user-ID, Facebook user-ID), username and website.

**Cookies**

Apps - just as web browsers - have the ability to set cookies and use web storage (together ‘cookies’).\(^{93}\) The NSHTTPCookie(Storage) class allows developers to set cookies for their apps.\(^{94}\) These cookies are invisible to users, as there is currently no way to view or delete them in iOS, unless apps provide the option to do so. It is safe to say that the majority of apps do not have such an option built-in. Cookies of apps can therefore - exceptions aside - only be deleted if an app is removed.

---

\(^{93}\) For more information on web storage see the World Wide Web Consortium: [http://dev.w3.org/html5/webstorage/](http://dev.w3.org/html5/webstorage/).

2.3 Methodology

To monitor the network traffic of apps, an iPhone 4S was purchased and set up as a new phone. This ensured that the device was not yet known to any third parties. The iPhone came pre-loaded with iOS 5.0, the latest version available by the time this research was conducted. A dedicated network environment was set up in order to ensure the accuracy of the collected data, and to prevent contamination thereof. Several other measures were taken as well:

- The spy Sinon, son of Aesimus, who told the Trojans that the wooden horse of the Greeks was a gift to the gods to ensure their safe return home, was used as a pseudonym during the research. The device name of the iPhone was set to ‘Sinon Aesimus’ iPhone’, while an e-mail address, a Facebook profile and a Twitter account were set up under the same name. These were used to interact with apps. In case apps required or offered a possibility to set up a user account, registration was performed using the same pseudonym and associated accounts.
- All apps were freshly installed on the iPhone from the App Store.
- Only one app was run at a time.
- The apps were used for a reasonable time, while exploring app specific features just as ‘regular’ users would. This included, *inter alia*, sharing content to social networks and tagging photos or messages with location data.
- Only the Wi-Fi connection of the iPhone was used. Cellular data was switched off.
- If an app required any form of consent or permission, it was given and noted.
- In order to capture the network traffic of the iPhone, a dedicated Wi-Fi network was created for the iPhone using a notebook and internet sharing. The network setup was as follows:
- The network traffic of the dedicated Wi-Fi connection was captured and analyzed using two tools. Burp Suite (version 1.4.01), which includes an intercepting proxy server, was used to capture HTTP/S traffic from the iPhone.95 The iPhone was manually setup to use this HTTP proxy.96 Wireshark (version 1.4.6), a free and open source network protocol analyzer, was used to capture non-HTTP/S traffic as well.97

---

96 A proxy in this case acts as an intermediary for data transfer between the iPhone and an external server.
In order to capture secure communications using the Secure Socket Layer (‘SSL’) with Burp Suite, a self-signed Certificate Authority certificate was authorized on the iPhone. Each time an HTTPS connection was made with a host, Burp Suite automatically generated certificates that were signed by the above mentioned Certificate Authority, for that specific host. This essentially provides a way to inspect secured communications traveling between the iPhone and the external host, before they are forwarded to the external host. The proxy acted as if it the data was directly send from the iPhone, and no eavesdropping had taken place.

The types of data collected during the monitoring of network traffic ranged from merely technical data and content, to possibly personal data. While collecting data, no focus was set on whether the data constituted personal data under the Data Protection Directive. Furthermore, no data was filtered out except content related data. Therefore merely technical data such as the device model, or the locale of the device is included as well.

For more information about this process see <http://portswigger.net/burp/help/servercerts.html>.

Fig. 2.5 Setup for network traffic monitoring
2.4 Results

The apps that were subject to this research were partially arbitrarily chosen. Some apps however were chosen because they are popular (e.g. Instagram, NU), or could have privacy risks that are reasonably foreseeable (Dosecast). The following apps were part of the research.99

TVGiDS.tv and TVGiDS.tv Lite are apps that provide Dutch television listings. Instagram is a social photo sharing app that lets users take photos, with the possibility of geotagging or applying effect filters to photos. Users can share their photos with friends or on social networks. NU is the app of the Dutch news website nu.nl, and offers users the latest news and headlines. Dosecast is an app that reminds its users to take their medications. Angry Birds Free, Little Lost Chick HD Lite and Blood & Glory are games.

Not all results will be discussed in-depth, instead one app - Instagram - has been chosen to demonstrate the results of the research. The rest of the results will be summarized, while the full results can be found in Appendix A.

Instagram

The Instagram app describes itself as “fast beautiful photo sharing for your iPhone”.100 It requires users to sign up with an account, after which they can take photos (or select already taken photos). Users can optionally edit their photos with ‘filters’, or add captions, hashtags, and location data. Photos of users are published on their Instagram feed, but can also be shared to a number of social networking sites (e.g. Twitter, Facebook, Flickr and Foursquare). Users can furthermore ‘friend’ and ‘follow’ other users to view their photos. Photos published on Instagram are public by default, while an option to keep photos private exists. In ‘private mode’ photos are only viewable by ‘friends’ of users.


100 See the Instagram website at <http://www.instagram.com>.
**Application:** Instagram

**Publisher:** Burbn Inc.

**iTunes link:** <http://itunes.apple.com/gb/app/instagram/id389801252?mt=8>

**EULA:** Available in-app and at <http://instagram.com/legal/terms/>

**Privacy policy:** Available in-app and at <http://instagram.com/legal/privacy/>

<table>
<thead>
<tr>
<th>Data</th>
<th>Payload</th>
<th>Permission</th>
<th>Remote host</th>
<th>Hostname</th>
<th>SSL</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDID</td>
<td>159701f3e17e51636a05*</td>
<td>No</td>
<td>50.17.241.161</td>
<td><a href="https://instagram.com">https://instagram.com</a></td>
<td>Yes</td>
</tr>
<tr>
<td>Location</td>
<td>(50.x, 14.x)</td>
<td>Yes</td>
<td>107.20.171.109</td>
<td><a href="https://api.foursquare.com">https://api.foursquare.com</a></td>
<td>Yes</td>
</tr>
<tr>
<td>Location</td>
<td>(50.x, 14.x)</td>
<td>Yes</td>
<td>50.17.241.161</td>
<td><a href="https://instagram.com">https://instagram.com</a></td>
<td>Yes</td>
</tr>
<tr>
<td>Address book</td>
<td>First, Last, E-mail, Numbers</td>
<td>No</td>
<td>50.17.241.161</td>
<td><a href="https://instagram.com">https://instagram.com</a></td>
<td>Yes</td>
</tr>
<tr>
<td>Phone number</td>
<td>+316*</td>
<td>Optional</td>
<td>50.17.241.161</td>
<td><a href="https://instagram.com">https://instagram.com</a></td>
<td>Yes</td>
</tr>
<tr>
<td>E-mail</td>
<td><a href="mailto:sinon.aesimus@gmail.com">sinon.aesimus@gmail.com</a></td>
<td>User</td>
<td>50.17.241.161</td>
<td><a href="https://instagram.com">https://instagram.com</a></td>
<td>Yes</td>
</tr>
<tr>
<td>Username</td>
<td>sinon.aesimus</td>
<td>User</td>
<td>50.17.241.161</td>
<td><a href="https://instagram.com">https://instagram.com</a></td>
<td>Yes</td>
</tr>
<tr>
<td>First name</td>
<td>Sinon</td>
<td>Optional</td>
<td>50.17.241.161</td>
<td><a href="https://instagram.com">https://instagram.com</a></td>
<td>Yes</td>
</tr>
<tr>
<td>Last name</td>
<td>Aesimus</td>
<td>Optional</td>
<td>50.17.241.161</td>
<td><a href="https://instagram.com">https://instagram.com</a></td>
<td>Yes</td>
</tr>
<tr>
<td>Gender</td>
<td>Male</td>
<td>Optional</td>
<td>50.17.241.161</td>
<td><a href="https://instagram.com">https://instagram.com</a></td>
<td>Yes</td>
</tr>
<tr>
<td>Website</td>
<td>sinon.aesimus.com</td>
<td>Optional</td>
<td>50.17.241.161</td>
<td><a href="https://instagram.com">https://instagram.com</a></td>
<td>Yes</td>
</tr>
<tr>
<td>Profile picture</td>
<td>-</td>
<td>Optional</td>
<td>50.17.241.161</td>
<td><a href="https://instagram.com">https://instagram.com</a></td>
<td>Yes</td>
</tr>
<tr>
<td>Twitter ID</td>
<td>SinonAesimus</td>
<td>Optional</td>
<td>50.17.241.161</td>
<td><a href="https://instagram.com">https://instagram.com</a></td>
<td>No</td>
</tr>
<tr>
<td>Device model</td>
<td>iPhone4, 1</td>
<td>No</td>
<td>69.63.189.63</td>
<td><a href="http://touch.facebook.com">http://touch.facebook.com</a></td>
<td>No</td>
</tr>
<tr>
<td>OS version</td>
<td>5.0</td>
<td>No</td>
<td>69.63.189.63</td>
<td><a href="http://touch.facebook.com">http://touch.facebook.com</a></td>
<td>No</td>
</tr>
<tr>
<td>OS</td>
<td>iPhone OS</td>
<td>No</td>
<td>69.63.189.63</td>
<td><a href="http://touch.facebook.com">http://touch.facebook.com</a></td>
<td>No</td>
</tr>
<tr>
<td>Carrier name</td>
<td>vfnl (Vodafone NL)</td>
<td>No</td>
<td>69.63.189.63</td>
<td><a href="http://touch.facebook.com">http://touch.facebook.com</a></td>
<td>No</td>
</tr>
</tbody>
</table>

**Fig. 2.6 Instagram**

On Instagram’s iTunes description page, no EULA or privacy policy is provided to users. A link to Instagram’s website can be found in the description, where users can navigate to the EULA and the privacy policy of Instagram. Upon the first use of the app, users are presented with the option to sign up for an Instagram account. During registration, no EULA or privacy policy is presented to users. After signing up however, users can find the EULA and the privacy policy within the app.

---

101 **Table explanation**

*Data:* The type of data that was processed.

*Payload:* The actual data that was sent to the receiving host.

*Permission:* This concerns permission. Yes represents that permission was asked and granted. No represent that no permission was asked and thus no permission was and could be granted. User represents user-entered obliged data. Optional represents user-entered optional data.

*Remote host:* The IP-address of the receiving host.

*Hostname:* The local hostname and domain name of the host in a HTTP(S)-header.

*SSL:* Whether the connection was secured with SSL.
When signing up for an account, an e-mail address and username is required. A phone number and profile picture is optional. The profile of a user can - after signing up - be edited to include a first and last name, a website, a short biography, a date of birth and gender. User-entered data is not visibly transmitted to third parties by Instagram.

Users have the option to encourage friends to use Instagram, by sending them invitations. They can also opt to find friends that already use Instagram with the help of their address book, or by linking their Twitter and Facebook accounts. The option to find friends by linking Twitter and Facebook accounts within Instagram, requires affirmative action from users by logging in to Twitter and Facebook. The option to find friends with the use of the address book however, required merely the tap of a button. When the option ‘Find Friends’ and subsequently ‘From my contact list’ was selected, Instagram uploaded the first and last names, e-mail addresses and phone numbers of all contacts to their servers. There was no further explanation, nor was there a pop-up that informed what was about to be happening. Merely tapping the ‘From my contact list’ option sufficed. No mention of this practice was made in their privacy policy. After the Path debacle, Instagram issued an update to the app. Choosing the ‘From my contact list’ option now prompts the user for permission with the following explanation: “Search for Your Friends in Address Book? - In order to find your friends, we need to send address book information to Instagram’s servers using a secure connection”.

In case users link their Twitter account to Instagram for automatic publications or finding friends, the Twitter ID (username) is retained. Upon linking a Facebook account, Facebook retrieves technical data about the device, as can be seen in figure 2.6.

For the use of location services by Instagram, the permission of users is required per the standard location permission pop-up found in iOS. Instagram uses the Foursquare API in order to retrieve venues in close proximity of the user’s location, and therefore transmits the user’s location data to Foursquare. No other data concerning users is sent to the Foursquare API besides location coordinates.

Finally the UDID of the device is processed, and cookies are set on the device. Several cookies were placed by Instagram, Facebook and Twitter.

---

102 Infra §4.1.3.1.
2.5 Summary

The TVGiDS.tv and TVGiDS.tv Lite apps are published by Mobile Pioneers (see figures A.1 & A.2, Appendix A). Both apps are licensed with the LAEULA and have a privacy policy available within the app. The apps process device names (‘Sinon Aesimus’ iPhone’) and UDIDs, and transmit them to an analytics company and several advertising companies. The payload shows that the ‘original’ UDID that is retrievable with the UIDevice API is used, alongside another UDID of which the computation is unknown. The privacy policy found inside the TVGiDS.tv Lite app, which consists of one sentence, mentions that the use of the app is completely anonymous. The TVGiDS.tv app has a more extensive privacy policy. It mentions the use of the UDID for statistics, personal preferences inside the app, ‘push notifications’ and technical support. TVGiDS.tv specifically mentions that the UDID is never connected to individuals, and that the UDID is not transmitted to third parties. The results show that the latter assertion is false, as the UDID is transmitted to several third parties. The privacy policy furthermore does not mention the use of the device name.

NU, the app of news website nu.nl, is published by Peperzaken (see figure A.3). The app processes UDIDs and location data. Upon opening the app the first time after installation, it prompts the user for permission to use location data. The purpose thereof is unknown, as it is not specified. The UDIDs that are processed by NU are transmitted to one analytics and one advertisement company. The latter also receives the location data of the user, possibly for location based advertising. The app has no privacy policy available inside the app. A privacy policy can be found on nu.nl, but it does not mention the mobile app, and thus the processing of UDIDs and location data.

Dosecast, published by Montuno Software LLC, is an app that helps its users to take their medication on time (see figure A.4). Users have the ability to specify, inter alia, their medications, the dosage, their doctor and their apothecary. Dosecast has implemented its own EULA that is available on iTunes. Users furthermore have to explicitly accept the EULA upon their first use of the app; declination results in not being able to use the app. The EULA, and the privacy policy found within, of Dosecast mentions that no ‘personally identifiable information’ is collected during the operation of the app. Dosecast processes UDIDs and any other data that is
entered by users about their medication. Dosecast has not been found to visibly share data with third parties.\textsuperscript{103}

Angry Birds Free, published by Rovio Mobile Ltd., is a free version of one of the most popular games available on iOS (see figure A.5). Angry Birds Free provides links to the EULA and privacy policy of Rovio in its iTunes description page. The EULA of Rovio is however not incorporated in the designated area in iTunes: according to the iTunes Connect Developer Guide, this leads to the app being licensed with the standard LAEULA.\textsuperscript{104} A link to the privacy policy is also available within the app. The privacy policy mentions that ‘non-personal data’ such as the UDID or IP-address is processed, and subsequently shared with ‘partners and contractors’ for analytics and advertisement purposes. The UDID is transmitted to one analytics company and six advertising companies, while the IP-address is shared with nine advertising companies. Three different payloads for the UDID were found; the original UDID provided by Apple, and two other UDIDs of which the computation is unknown.

Little Lost Chick HD Lite, published by Clickgamer Technologies Ltd., is licensed with the LAEULA (see figure A.6). Clickgamer does not provide a privacy policy within the app, nor can a privacy policy be found on its website. Little Lost Chick implements the social gaming platform Crystal, which is operated by Chillingo Ltd. Crystal allows players to unlock achievements, view leader boards and share high scores to social media. The use of Crystal requires a Crystal account. During the sign up process, the terms and conditions and privacy policy of the Crystal service can be viewed by users. The privacy policy mentions that Crystal collects names, photos or avatars, e-mail addresses, geolocations, UDIDs and IP-addresses of users. That data is indeed processed, in addition to users’ Facebook IDs, GameCenter IDs and address books, in case they choose to ‘connect’ with friends. The UDIDs of users are furthermore collected even if users do not have a Crystal account, or a fortiori have not even interacted with Crystal at all.

Blood and Glory, published by Glu Games Inc., is a game where one assumes the role of a Roman gladiator (see figure A.7). The app provides its own EULA in iTunes, and provides a

\textsuperscript{103} Data might be shared with third parties, but this does not happen automatically during the use of the app.
link to its privacy policy within the EULA. Both documents are also available through a link within the app, and on the website of the publisher. The privacy policy of Glu explains what data is processed by Glu, and third parties that Glu collaborates with. The third-party services are mentioned specifically and include, *inter alia*, Facebook, Flurry Analytics, Playhaven Advertisement and OpenFeint social gaming. Blood and Glory was observed to transmit the UDID to one analytics, one social gaming and three advertising companies. One advertisement company also retrieved the MAC-address of the device, while a social gaming platform also retrieved the device name.

Regarding the privacy policies and EULAs of the researched apps, the following conclusions can be drawn: six out of the eight observed apps had privacy policies available from within the app, while two apps had no privacy policy. Five out of eight apps were licensed with the LAEULA. Of the three other apps, one explicitly required acceptance of their EULA from users.

<table>
<thead>
<tr>
<th>Application</th>
<th>In-app</th>
<th>Website</th>
<th>EULA</th>
<th>LAEULA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instagram</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>TVGiDS.tv</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>TVGiDS.tv Lite</td>
<td>Yes1</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>NU</td>
<td>No</td>
<td>Yes2</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Dosecast</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Angry Birds Free</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Little Lost Chick</td>
<td>No3</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Blood and Honor</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Fig. 2.7 Availability of Privacy Policies

1: The privacy policy mentions that the use of the application is completely anonymous.
2: There is a privacy policy available on their website, but it does not mention the use of or data processed by the application.
3: There is however a privacy policy available within the app of the social gaming network Crystal.

Of course merely implementing a privacy policy does not make the processing of personal data legitimate. A closer look will be taken at some of the privacy policies of these apps in chapter four.
2.6 Conclusion

The checks and balances to control the amount of data accessible - and the accessibility itself by developers - differs per platform. The iOS SDK provides an API where developers can get access to a dataset that is predefined by Apple. Prior permission from users, in the form of a pop-up, is only required when an app wants to access location data. Misuse of accessible data is sought to be prevented by an ex-ante review of apps, in combination with the enforcement of rules that are set out in the App Store Review Guidelines. Google has a different approach: apps are reviewed ex-post, while access to data is handled by a permission model. The permission model requires developers to request permissions from users to use features of SMDs or to access data. In contrast to iOS, Android allows developers to gain access to a lot more data. A list of permissions to access data, including a brief description of the sought permissions by Google, is presented to users prior to the installation of an app, which they can accept or decline.

The amount of available and accessible data in the iOS SDK is substantial. Developers have access to a wide array of data: the majority of the time without having to request prior permission from users. This includes - most notably - address books, calendars, device names, location data, photos and UDIDs.

Monitoring the network traffic of apps showed a glimpse of what data is actively and passively processed by apps. As can be seen in the results, users are not always informed of the data that is processed or subsequently shared with third parties. The most notable processing in the results was the address books of users by the Instagram app. Neither in their privacy policy, nor during the process itself, are users made aware of the fact that their address book is transmitted to the servers of Instagram.
3. Applicable Laws and Jurisdiction

“Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. [...]”

- Article 8 of the Charter of Fundamental Rights of the European Union

This chapter has the primary goal of discussing the applicability and jurisdiction of the Data Protection Directive (‘Directive’) and the e-Privacy Directive with regard to apps. The phrase ‘applicability’ is used to indicate whether apps fall within the substantive scope of the directives, while ‘jurisdiction’ in this chapter denotes the fact whether the directives, and thus subsequently national data protection laws of Member States, are applicable to apps.

First, the applicability of the Data Protection Directive is analyzed. The main question in this paragraph is whether apps process personal data, and will include an evaluation of available data on SMDs under the concept of personal data. Second, the jurisdiction of the Data Protection Directive is discussed. This paragraph will elaborate on data controllers of apps. The focus will furthermore be set on whether the Data Protection Directive has jurisdiction over data controllers of apps, that have no relevant establishment within the European Union (‘EU’): jurisdictional issues will foremost play a role with data controllers of apps that are not established within the EU.105 Finally, the applicability and jurisdiction of the e-Privacy Directive is analyzed. The focus in this paragraph is set on whether article 5 (3) is applicable to apps.

Throughout this chapter, the directives are the focal point, and not the specific implementations of the directives in Member States. This will be similar regarding the jurisdictional scope of the directives; no focus will be set on which national law specifically applies. Rather the fact whether any national law applies is analyzed, because of the vast territorial diffusion of publishers of apps. Furthermore, the opinions of the Article 29 Working

---

105 Where ‘EU’ is used, it is interchangeable with ‘Community’, and also includes the European Economic Area.
Party (‘Working Party’) are taken into account when discussing the directives.\textsuperscript{106} Finally, where suitable, results from the research on apps of chapter two will be evaluated.

### 3.1 Applicability of the Data Protection Directive

The Data Protection Directive forms the fundament to the lawful processing of personal data within the EU, and aims to protect individuals.\textsuperscript{107} The substantive scope of the Directive is applicable when ‘personal data’ is ‘processed’.\textsuperscript{108}

**Personal data**

Personal data is defined in the Directive as “any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity”.\textsuperscript{109} The definition consists of four components which can be disseminated as follows: (1) “any information”, (2) “relating to”, (3) “an identified or identifiable” and (4) “natural person”. These components will be successively discussed.

In its opinion “on the concept of personal data”, the Working Party has elaborated on the four components of the definition of personal data.\textsuperscript{110} The wording of “any information” per se is very broad, in the sense that it could indeed cover any sort of information.\textsuperscript{111} The Working Party states that from the point of view of the nature of the information, both ‘subjective’ and ‘objective’ information is covered. The format of the information can be in any form; even binary code stored in the memory of a device.\textsuperscript{112}

\textsuperscript{106} The Article 29 Working Party is an independent EU advisory body set up under article 29 of the Data Protection Directive. It advises Member States and the European Commission on data protection matters, promotes the uniform application of the general principles of the directives, and publishes explanatory opinions. The Working Party, \textit{inter alia}, consists of representatives of Data Protection Authorities from all Member States. See \url{http://ec.europa.eu/justice/data-protection/article-29/index_en.htm}.

\textsuperscript{107} Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

\textsuperscript{108} Article 3 Data Protection Directive; Schnabel 2009, p. 517.

\textsuperscript{109} Article 2 (a) Data Protection Directive.


Whether information “relates to” an individual, can be determined using three non-cumulative elements: content, purpose and result.\textsuperscript{113} The content element covers information about an individual, regardless of the purpose of a data controller or the impact it has on a data subject.\textsuperscript{114} In the light of apps, this could for example be the locale or country code of a SMD. They can denote the country of residence of a user, assuming that it can be linked to an individual. The purpose element can relate information to an individual if the data is used to evaluate or influence the status or behavior of an individual. From the point of view of apps, the unique device identifier (‘UDID’) can be an example of data that could have the purpose to evaluate an individual, as the UDID can be used by analytics and advertising companies to profile users across apps. Finally, the result element covers data that is used to impact, however big or small, an individual’s rights or interests. The Working Party states that for the result element, it is sufficient that an individual is treated differently from others.\textsuperscript{115} The above mentioned UDID is a good example of the possible cumulation of the three elements. The UDID is information about a user as it is tied to the user’s device. It can be used for the purpose of profiling the user, and it can have the result that a user is shown different advertisements based on their profile that is generated with the use of the UDID.

The Directive makes a distinction between an identified or identifiable person. While an identified person is intrinsically identified, the concept of an identifiable person presumes the possibility to identify a person. This possibility can present itself through direct or indirect identifiability. Direct identifiability may be achieved, \textit{inter alia}, by the name of an individual, depending on the circumstances of the case and given that one would be able to distinguish the individual from other individuals. Indirect identifiability can be caused by data that has unique characteristics (‘CEO of Google Inc.’), or by combining data that per se does not identify an individual, but when combined with other data, could lead to the identification of an individual.\textsuperscript{116} In this regard it is not necessary for the concept of an ‘identifiable person’ to identify an individual by its name; the ability to single out an individual from others with the use

\begin{footnotesize}
\begin{enumerate}
\item \textsuperscript{113} Idem, p. 10.
\item \textsuperscript{114} Nouwt 2008, p. 385.
\item \textsuperscript{115} WP Opinion 4/2007, p. 11.
\item \textsuperscript{116} Kuner 2007, p. 92; Nouwt 2008, p. 385.
\end{enumerate}
\end{footnotesize}
of an identifier can be sufficient for indirect identifiability.\textsuperscript{117} An example of this concept is the use of cookies with unique identifiers, that are used to single out and target individuals.\textsuperscript{118} The recital of the Directive mentions that all means that are likely reasonably to be used by a data controller or third party to identify a person should be borne in mind, when determining whether a person is identifiable.\textsuperscript{119} A relevant factor worth mentioning in this context is the purpose of the data processing; when prima facie not identifiable data is processed with the purpose to single out and target individuals, one can hardly argue that those individuals are not identifiable, albeit not directly.

Regarding the last component of the definition of personal data, for the purpose and scope of this chapter, the assumption that users of smart mobile devices are indeed (living) individuals is sufficient.

\textit{Personal data and apps}

The previous chapter gave a good overview of the kinds of data that can be processed by apps on the iOS mobile operating system of Apple. This list is limited to iOS, as other mobile operating systems may offer wider access to data. Nevertheless, the available data on iOS will certainly overlap with other mobile operating systems, and can accurately demonstrate what kind of data is available on smart mobile devices.

Naturally, not all apps process personal data. Similarly, not all data that is processed by apps can be qualified as personal data. Some types of data, like the timezone or the language of a device, say little about an individual. However, when they are combined with other data, they can enhance the identifiability of a user. Since there is no common standard of what data apps process, it will ultimately depend on the circumstances of the case whether personal data is processed by an app. The following paragraphs will evaluate whether the available data on iOS - as discussed in chapter two - constitute personal data under the Data Protection Directive. The available data are discussed individually, largely following the structure of §2.2

\textsuperscript{119} Recital 26 Data Protection Directive.
Technical data

The data that was collected by apps in chapter two shows that a range of technical data is processed by apps. Most notably, with the concept of personal data in mind, is the processing of IP-addresses, device names, UDIDs and MAC-addresses. However, information about a user’s carrier, timezone or locale should not be discarded as irrelevant. While they might not constitute personal data per se, they are relevant information when combined with other personal data. They could denote the country of residence of users by utilizing the details of the timezone, the users’ subscribed carriers and the language they prefer, although that information is not always necessarily correct.\(^\text{120}\)

When apps transmit data, the IP-address of the device is naturally transmitted because of the Internet Protocol. The IP-address can also be locally detected on the device, or derived from the HTTP-requests made from the device. There seems to be a consensus within the EU that IP-addresses constitute personal data, or at least have to be treated as such, as subscribers are indirectly identifiable by their Internet Access Provider.\(^\text{121}\)

Device names could constitute personal data, especially in the default state. In case users do not change their device names, the default name is set to the first and last name of the Apple ID of users. The same applies to the GameCenter ID of users, which, although it is not set to the first and last name of users by default, could contain the real name of users. While a common name alone can not directly identify an individual, names that are unique could certainly do so. A common name could also identify an individual if it is combined with other available data (e.g. date of birth and timezone which can denote the user’s country of residence).

The UDID is intrinsically the ultimate tracking tool present on iDevices. Similar to tracking cookies, it is a tool that specifically allows the tracking of users on smart mobile devices. Unlike cookies though, the UDID can not be deleted or altered by users. It is also not possible for users to control access to the UDID by apps or any subsequent transmission to third parties by apps. It is therefore no surprise that the use of the UDIDs by apps and the transmission

\(^{120}\) My device for example deliberately has the timezone of another European city than the one I reside in, albeit one that is in the same timezone. I have been roaming with my carrier for a long time, while the carrier data reflects the SIM-card that is in use. Finally I prefer to use English on my devices instead of my native tongue.

of UDIDs to analytics and advertising companies is widespread. It is the ultimate tool for publishers, and advertisement or analytics companies, to track users. In the case of analytics and advertising companies, the UDID even allows them to track users across apps. They can furthermore use the UDIDs to build profiles of users based on the apps they use and any further information they can tie to a specific UDID (e.g. location data, age).

The key to detailed user profiles is data. The more data there is, the more detailed a profile will be.\textsuperscript{122} If an analytics or advertisement company receives data from tens of thousands of apps, which is not unrealistic based on the amount of apps available in application catalogs, detailed profiles can be made of users that can be used for behavioral advertising. One of the biggest analytics providers on smart mobile devices, Flurry Inc., currently serves more than 60,000 companies with over 150,000 apps across all mobile platforms.\textsuperscript{123} According to their privacy policy, they tie UDIDs to Flurry IDs.\textsuperscript{124} The fact that the tracking of users is achieved through the use of the UDID, is positively proven by the fact that Flurry - and other companies - give users the ability to opt-out of tracking with their UDIDs.\textsuperscript{125} The tracking and profiling of users allows Flurry to display information to publishers of apps about, \textit{inter alia}, their users’ categories of interest, location, language and estimated gender.

The amount of profiling that can be achieved is immense. Imagine a user that has the following apps installed on his device: The Democrats, iBaby Monitor, The Torah Bible Pentateuch, Cancer Signs and Symptoms, Chopin Waltz & Impromptus and 3in1 Mortgage Calc. Assume that all of these apps send the UDID of the user’s device to an advertisement company. While these apps individually have no significant meaning regarding profiling, the combination of them does. One can likely infer - whether correct or not - that the individual behind the profile based on these apps is a democrat, a father or mother of at least one child or in expectance thereof, and is of jewish religion or at least interested in the subject. The individual furthermore may have cancer, is in fear thereof, or is interested in the subject, likes classical music and owns real estate or is interested in it.

\textsuperscript{122} Cleff 2007, p. 228.
In March 2012, seven months after announcing the deprecation of the UDID, Apple has slowly started to reject apps that use the UDID.126 Developers, analytics and advertising companies have not been idle in the meanwhile and have been working on new ways to keep tracking users. Several alternatives for the UDID that is provided by Apple have been developed.127 Some developers sought their refuge in using the MAC-address of iDevices as a UDID, while other initiatives in the form of ready-made software that can produce UDIDs have been developed.128 This ongoing process can also be seen in the results from chapter two, as different UDIDs are processed.

The UDID is used by apps, analytics and advertising companies to single out users for different purposes. While apps might single out users because it is necessary to distinguish users for the services provided by the app, they are not prevented from using any unique identifiers at all. While Apple has deprecated the use of the UDID, it does offer developers to generate app specific UDIDs. This ‘app UDID’ will tailor to the most needs of developers, while it does not have the specific privacy risks of the UDID. The UDID can furthermore have the purpose to evaluate individuals - as used by apps and analytics companies - or to influence the behavior of individuals - as used by advertising companies that present targeted advertisements.

The deprecation of the UDID hits the analytics and advertising companies the hardest, as they have to find alternatives to keep tracking users across apps and to measure the effectiveness of their advertisements. It furthermore also leads to lower prices paid out to publishers of apps that rely on advertisement.129 The Working Party is of the opinion that unique identifiers of smart mobile devices constitute personal data, because users can be singled out.130 UDIDs can also be tied to other data like e-mail addresses or (user)names provided to an app by its users. Some analytics and advertising companies even offer developers the ability to send location data,
usernames, e-mail addresses or other demographical information. Furthermore, to tie a UDID to an identified person, it is sufficient that it is combined with identifying personal data.

While the UDID could constitute personal data by itself due to its ability to single out individuals, a subject access request to iTunes s.a.r.l. in Luxembourg by yours truly provided evidence that the UDID of an iDevice is linked to the Apple ID of its user. Every time users download an app from the App Store, their UDID and IP-address are processed alongside their Apple ID. The Apple ID contains personal data like names, addresses and financial information, that are required to make purchases in the App Store. The UDID is therefore linked to an directly identifiable individual, and can be used to indirectly identify an individual by combining it with personal data controlled by iTunes s.a.r.l. This is a similar situation to the above mentioned IP-address.

The UDID can thus be qualified as personal data on two grounds. Firstly, because of the fact that the UDID can single out users. Secondly because users are indirectly identifiable when the UDID is combined with personal data that is controlled by iTunes s.a.r.l.

**On-device data**

The address book, calendar, location services and photos of users can reveal intricate details. The address book by definition contains personal data in the form of names, e-mail addresses and phone numbers, and will mostly contain data regarding identified individuals. Whether the calendar of users constitutes personal data per se, depends on the entries made in the calendar and thus on the circumstances of the case. It is safe to presume though that calendars can contain personal data when the calendar entries are detailed, and include a description of names and location of an appointment. The calendar could, and especially when combined with other identifying personal data should, therefore be regarded as personal data.

---

131 iTunes s.a.r.l. is a subsidiary of Apple Inc. and the controller of data subjects within the EU. See Apple’s privacy policy under ‘International Users’, available at [https://www.apple.com/privacy/](https://www.apple.com/privacy/). The subject access request was based on article 26 of the Luxembourg Data Protection Act.

132 An interesting question that will not be discussed is whether apps can receive consent from the user (to which the address book belongs) to process the personal data of the people that are in the address book, as it is primarily the personal data of the *contacts* that are being processed, and not of the user itself.
Photos with portraits are personal data if it is possible to directly identify an individual.\(^{133}\)

In some countries, like the Netherlands, portraits are even considered to be *sensitive* personal data under section three of the Directive, because one can deduce the racial or ethnic origin of the portrayed individual(s).\(^{134}\) Although not all photos on smart mobile devices necessarily have individuals portrayed in them, the likelihood is significant. Even if not all photos automatically constitute personal data, and disregarding the fact that it is hard - if not impossible - to technically guarantee whether a photo library contains portrayed individuals, especially when photos are combined with other identifying personal data, they should be regarded as such, because they are information relating to an individual.

Location services can pinpoint the exact location of an individual. The Working Party accurately demonstrates the fact that location services can give an intimate overview of the habits and patterns of a user, especially when a large sample of location data about a user is at hand.\(^{135}\) The effect of large samples of location data was demonstrated by the German politician Malte Spitz, when he collaborated with the newspaper Zeit and published his location data spanning over a period of six months.\(^{136}\) The fact that location data can give an intimate overview of the habits of a user, was further demonstrated by the app ‘Girls Around Me’ on iOS.\(^{137}\) Girls Around Me showed its users a map with women (including available portraits) that were present around their location. The information was gathered through publicly available location and personal information on Foursquare and Facebook. After raised privacy concerns, Foursquare denied the developers of the app access to its API that was used to gather location data of women. This ultimately lead to the developer pulling the app from the App Store.\(^{138}\)

\(^{133}\) Kuner 2007, p. 92; WP Opinion 02/2012, p. 5.

\(^{134}\) Supreme Court of the Netherlands, 23 March 2010, LJN BK6331; Article 8 Data Protection Directive.


The fact that the e-Privacy Directive regulates the use of location data in the telecommunications sector, demonstrates that location data are seen to entail specific risks to privacy.\textsuperscript{139} The Working Party is of the opinion that location data of smart mobile devices, especially with repeated observations, should be considered personal data, because the owner of the device can be identified, especially when combined with indirect identifiers. While that might be correct, the assumption that location data per se, and in every circumstance, constitutes personal data is untenable. Not all processing of location data can be considered as the processing of personal data.\textsuperscript{140} If an app merely processes location data without any other identifiers, it cannot always be considered personal data. That being said, in the case of apps, as the results in chapter two show, the location data is often tied to the UDID of a device and/or other identifiers, which can indirectly lead to the identification of users. In those cases, when location data is combined with other identifiers that could lead to the identification of an individual, it should be considered personal data.

\textit{User-entered data}

Naturally any information can be collected by publishers, as long as data subjects are willing to disclose information. The nature of the collected data can be very diverse, ranging from social media usernames and phone numbers or date of births, to trivial information like favorite food or color. Whether user-entered data qualifies as personal data, depends on the circumstances of the case and the data that is processed. It has to be noted however, that user-entered data could raise risks due to the sensitive nature of the information. This can be demonstrated with the Dosecast app.

The Dosecast app reminds its users to take their medication. The collects information about the medication of its users, as discussed in §2.5. The Directive considers information about health to be sensitive data: a stricter regime applies to their processing.\textsuperscript{141} The privacy policy of Dosecast states that no ‘personally identifiable information’ is collected during the operation of the app. The app however processes the UDID alongside user-entered information about

\textsuperscript{139} Cuijpers & Koops 2008, p. 886.
\textsuperscript{140} Cuijpers & Koops 2008, p. 888; Schnabel 2009, p. 530.
\textsuperscript{141} Article 8 Data Protection Directive.
medications, and transmits them to Dosecast servers. When medical information of users are combined with their UDID, it is possible to indirectly identify the individuals that are using the app, and gain insight in to their health.

Processing of personal data
The second factor, “processing of personal data”, is broadly defined and enumerates many - if not all - operations that can be performed upon personal data.\textsuperscript{142} The enumeration consists, \textit{inter alia}, of collecting, storing and transmitting personal data. Whether the operations are performed by automatic means or not, does not matter. As a result, any operation performed upon personal data will most likely fall within its definition. This is no different for the processing of personal data by apps on smart mobile devices. Whether apps are collecting, storing, or transmitting personal data on or from smart mobile devices, their operations fall within the definition of “processing” in the Directive.

It can be concluded from the evaluation of the available data in this paragraph, that a majority of the data constitutes personal data. This also leads to the conclusion that all apps that have been researched in chapter two, processed personal data. While no hard conclusions can be drawn regarding all available apps in application catalogs, it is safe to presume that a majority processes personal data, and thus fall within the substantive scope of the Directive.

3.2 Jurisdiction and the Data Protection Directive
Although apps fall within the substantive scope of the Directive when they process personal data, the important question is whether the Directive has jurisdiction over publishers of apps. This question is especially interesting with regard to publishers of apps that are established outside the EU, and shall thus be the focus of this paragraph. Although no official figures exist, it is safe to assume that the amount of publishers that are established outside the EU is vastly more substantive than those that are established within the EU. This paragraph will first discuss the concept of data controller in the context of apps, followed by an analysis of the jurisdictional provisions of the Directive.

\textsuperscript{142} Article 2 (b) Data Protection Directive; Kuner 2007, p. 98.
In determining the jurisdictional scope of the Directive, the data controller plays a key role. A controller is defined in the Directive as “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”. The qualification of an actor as controller is important, as most obligations from the Directive must be met by the controller, and controllers are liable for data protection violations. Closely related to the controller is the processor: anybody who processes personal data on behalf of the controller. Regarding apps, in the majority of cases, the publisher is likely also the controller. There can be exceptions to this rule of thumb though.

Consider the following examples:

- an app is developed for X by a mobile development company. While X is the data controller, the app is published in an application catalog by the mobile development company;
- an app is published by X. X is a subsidiary of Y and they are joint controllers of the processed data;
- an app is published by X. X transmits personal data to analytics company A and advertisement company B. Depending on the circumstances, X, A and B can either be individual controllers, joint controllers or processors.

The given examples show that analytics and advertising companies can be data controllers. Although developers have to incorporate the SDKs of analytics and advertising companies, the latter can - and do - determine the purposes and means of the processing of personal data: they develop their own SDKs and can decide which personal data is being processed, and for what purposes. Apps can thus have multiple data controllers, especially when analytics and advertising companies are involved. In light of the above, it is important to establish on a case-by-case basis, who the controller is - or controllers are - of personal data processed by an app.

143 Article 4 Data Protection Directive.
144 Article 2 (d) Data Protection Directive.
145 Kuner 2007, p. 69.
146 Article 2 (2) Data Protection Directive.
147 From the definition of controller in the Data Protection Directive, it should be clear that even hobbyist developers that publish applications can be data controllers.
148 The exact relationship between analytics companies, advertising companies and publishers, and moreover whether they are (joint) data controllers and/or processors, falls outside the scope of this thesis.
For the sake of brevity, the above mentioned rule of thumb will hereinafter be followed. The phrase ‘publisher’ will therefore be used to denote data controllers of personal data that are processed by apps. It is however interchangeable with any actor that is a data controller of personal data that is processed by an app.

The jurisdictional scope of the Directive is regulated by article 4, and more specifically, since the Directive is implemented in the data protection laws of the Member States, which national law applies to a particular processing activity. The rationales behind the jurisdictional provisions of the Directive are twofold: firstly, to avoid gaps where no data protection laws would apply, secondly, to avoid multiple applications of national laws.149

The jurisdiction of the Directive can be triggered in two ways.150 First, when the processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of the Member State.151 Second, when the controller is not established on Community territory, but for the purposes of processing personal data makes use of equipment, automated or otherwise, that is situated on the territory of a Member State.152 An exception is made in the latter case, when the equipment is only used for purposes of transit through the territory of the Community. The Directives makes a distinction between controllers that are established within and outside the EU.

Article 4 (1) (a) is mostly relevant for publishers of apps that are established within the EU. While much has been said and written about which national law applies to a particular processing, especially when a controller has several establishments scattered throughout the EU, it is safe to assume that the Directive will have jurisdiction over publishers that are established within the EU. The more interesting question is whether the Directive has jurisdiction over publishers that are established outside the EU, and have no relevant establishment within the EU.

The rationale behind article 4 (1) (c) is the fact that individuals should not be without protection when their personal data is processed, even if the controller is not established on Community territory. The provision has two relevant components that will be discussed successively: (1) “the controller is not established on Community territory”, (2) “and for

150 Whether the Directive has jurisdiction by virtue of international public law, is not relevant for apps.
151 Article 4 (1) (a) Data Protection Directive.
152 Article 4 (1) (c) Data Protection Directive.
purposes of processing personal data makes use of equipment, automated or otherwise situated on the territory of the Member State”.  

The Working Party has touched on this subject in different opinions throughout the last decade. The first component requires that the controller is not established on Community territory. The notion of establishment is determined by the location where the controller has effective and real exercise of the processing activities, conforming to the interpretation by the Court of Justice of the European Union. For this chapter, it is assumed that non-EU based publishers have no relevant establishment in the EU that could trigger the application of article 4 (1) (a), as article 4 (1) (c) only applies when the first does not. When such a relevant establishment does exist, further analysis is required to determine whether the Directive has jurisdiction on the basis of article 4 (1) (a) or (c).

Whether apps, and the smart mobile devices they are used on, are equipment is an interesting question. As Kuner points out, when the Directive was adopted in 1995 - before the widespread use of the internet, let alone smart mobile devices - the term equipment was probably not foreseen to be of as great importance as it is now. Perhaps that is why the Working Party advocated a cautious approach to apply this provision. Only in cases where it is necessary, it makes sense and where there is a reasonable degree of enforceability - to prevent over-application that could have negative practical consequences - should the provision be applied. In later opinions though, the Working Party favors a wider scope of its application, while still recognizing possible unsatisfactory consequences.

The Working Party has put forward the view that equipment should be at the disposal of the controller for the processing of personal data. No full control of the equipment is required, nor property or ownership. Instead, whether the controller can determine what data is processed and for which purposes, should be considered. This implies two elements: action taken by the

153 The third component, exemption for purposes of transit only, is not discussed in this chapter as it is irrelevant to apps.
157 Kuner 2007, p. 120.
158 WP International application, p. 9.
160 Idem.
controller and the intention to process personal data. In its earlier opinions the Working Party qualified the use of cookies and JavaScript as “making use of equipment”, because a user’s PC qualifies as equipment.\textsuperscript{161} In a later opinion the Working Party qualified smart mobile devices that are used by a controller to provide geo-location services through dedicated software installed on the device, as equipment.\textsuperscript{162}

Apps are software that are inherently linked to smart mobile devices, as without it, they can not function. The question whether apps per se can be considered as equipment can be ignored, since the SMDs they are installed on and utilize, should certainly be qualified as equipment. Publishers do not have full control of the SMDs of users, nor do they own them, but they do have the SMDs at their disposal to process personal data with their app. They can determine which personal data is processed and for what purposes, as they have control over how their app functions and which data it collects.

There are millions of European users that use apps on their smart mobile device within Community territory. A majority of these apps are published by publishers of apps that are not established within the EU. Therefore, not qualifying smart mobile devices as equipment would create a severe lacuna in the protection of their personal data and the application of the Directive. As such, the Data Protection Directive should also apply to publishers of apps that are not established - and have no relevant establishment - within the EU.

That being said, a consequence of the applicability of article 4 (1) (c) is that publishers most likely will have to comply with multiple data protection laws.\textsuperscript{163} Publishers are furthermore obliged to designate a representative that is established on the territory of each Member State whom’s national law is applicable, which can be a burden.\textsuperscript{164} Kuner puts his finger on the problem of enforceability.\textsuperscript{165} While he criticizes the assertion of jurisdiction that the EU “can not hope to enforce” and that would undermine general respect for data protection law, denying the applicability of the Directive on apps would undermine the goals of data protection law itself: the protection of individuals with regard to the processing of personal data. The desirability or

\begin{enumerate}
\item Supra note 159.
\item In this regard also see WP Opinion 1/2008, p. 11.
\item Article 4 (2) Data Protection Directive; Kuner 2007, p. 131.
\item Kuner 2007, p. 125.
\end{enumerate}
practicality of these consequences and enforcement issues can be subject to discussion, but fall outside the scope of this paragraph.166

3.3 Applicability of the e-Privacy Directive

The e-Privacy Directive can be characterized as a *lex specialis* to the Data Protection Directive, as it specifically covers data protection in the electric communications sector. The e-Privacy Directive complements the Data Protection Directive, where as the latter applies to all matters that are not specifically covered by the e-Privacy Directive.167

The scope of the e-Privacy Directive limits its applicability to publicly available electronic communications services in public communications networks within the Community.168 Some provisions of the e-Privacy Directive however are more widely applicable, and are not limited to electronic communication services.169 The most notable and relevant provision for apps is article 5 (3) of the e-Privacy Directive. Dubbed the ‘cookie article’, it has gained much attention, stirred up a lot of debate and generated a lot of confusion amongst stakeholders. Article 5 (3) of the e-Privacy Directive states that the storage of information, or gaining access to already stored information, in the terminal equipment of a user, is only allowed if the user has consented thereto, after being provided with clear and comprehensive information about the purposes of processing.170 An exception is made insofar technical access or storage is strictly necessary for the sole purpose of the transfer of communications, or to provide a service provided by an information society service that is explicitly requested by a user.171 In this paragraph the applicability of article 5 (3) to apps will be analyzed by successively discussing the following components of article 5 (3): (1) “terminal equipment”, (2) “information” and (3)

---

168 Article 3 e-Privacy Directive; Schnabel 2009, p. 521; Kuner 2007, p. 136;
170 For the definition of user see article 2 (a) e-Privacy Directive: “any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service”.
171 When accessed or stored information is strictly necessary to provide the services of an app, requires further analysis; it is difficult to answer this question *in abstracto* and falls outside the scope of this thesis.
“storing information or accessing already stored information”. Other components of article 5 (3), including consent and the obligation to inform users, will be discussed in §4.2.1.

A few general observations have to be made before discussing the aforementioned components. First, article 5 (3) is not only a framework for browsers and cookies. The recitals of the e-Privacy Directive provide examples of other objects that can be stored or accessed on the terminal equipment of users: spyware, web-bugs and hidden identifiers.172 These are confusingly referred to as ‘devices’. In the context of article 5 (3), devices are objects that are either meant to be stored or accessed on the terminal equipment of users. The nature of the object (e.g. spyware, cookies) denotes its further use. Secondly, the recitals of the e-Privacy Directive state the rationale behind article 5 (3): information that is stored on terminal equipment of users belongs to their private sphere which requires protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms. The recitals furthermore provide three examples of means that objects can use that can “seriously intrude upon the privacy of [...] users”: (1) third parties can gain access to information without the knowledge of users, (2) store hidden information, or (3) track the activities of users. The recitals also state that the above mentioned objects should only be used for legitimate reasons while users are informed about their presence.

Thirdly, article 5 (3) is applicable to any actor that stores or accesses information on the terminal equipment of users, irrespective of whether they are data controllers or data processors.173 Most relevant in this regard are information society services, as apps can be deemed to be such services.174 Finally, purposes for accessing or storing information on terminal equipment do not play a role in article 5 (3), save for the exception: the purpose of accessing or storing information is therefore irrelevant for its applicability.175

172 Recital 24 e-Privacy Directive.
174 For a definition of information society services, see article 1 (2) Directive 98/34/EC: “any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services”. Further clarification can be found in Annex V of Directive 98/34/EC and in recitals 17-18 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market. It is evident that apps fall within the definition and should be qualified as information society services.
175 Debuserre 2005, p. 84.
The definition of “terminal equipment” is broad, so that smart mobile devices fall within its definition. The e-Privacy Directive does not provide a definition of “information”. The Working Party has stated that “information” does not necessarily needs to be personal data. The recitals of the e-Privacy Directive support that interpretation, by stating that any information stored on terminal equipment of users are part of their private sphere. What follows however is a grey area regarding what information and technologies are covered by the provision. Debussere mentions that this vagueness undoubtedly corresponds to the intention of drafting the provision as technology-neutral as possible.

Apps can store, and more importantly, access all sorts of information as has been extensively discussed in chapter two. Data that are retrieved by apps, are often “already stored information”. When location data is retrieved realtime through GPS on the device, apps access information that is already stored on the device, as the location data has to be stored on the device before apps can retrieve that information. An address book of a user is similarly already stored information on the device.

Does an app that tries to access an address book fall within the scope of the provision? When compared to cookies and hidden identifiers, one is likely to say no, as apps are not similar objects. A negative answer however would undermine the rationale of the provision, as an address book is at the core of information stored on terminal equipment of users that should be regarded as falling in their private spheres.

By taking a look at the objects that are given as examples in the e-Privacy Directive, one can wonder whether apps belong in that list. Apps are generally not spyware, web-bugs, hidden identifiers or cookies. There are apps available however that could qualify as spyware or malware. The fact that spyware is considered as an example, proves however that software

---

179 Debussere 2005, p. 83.
(and thus also apps) can fall within the scope of article 5 (3). The recitals of the Citizens’ Rights Directive also states multiple ways (e.g. “downloaded via electric communications networks”) of how software can be acquired by a user, and disregards the manner in which the software is acquired for the protection of users.\textsuperscript{181} There is therefore no reason why apps that are downloaded from application catalogs would fall outside its scope.

In the context of cookies, the personal computer of a user is the terminal equipment, while websites access or store information (e.g. cookies) with the help of a browser. Analogizing this to apps results in the following: the smart mobile device of a user is the terminal equipment, while apps access or store information with the help of a mobile operating system.\textsuperscript{182} An app is therefore the same kind of object, and on the same level, as websites that utilize cookies, or spyware that is stored on and accesses a user’s terminal equipment.

To make things more complicated - or easy if you will: apps also store and access cookies on smart mobile devices, as discussed in chapter two.\textsuperscript{183} Unlike browsers however, users generally do not have the option to block, view or delete cookies that are stored and accessed by apps. On iOS for example, users can only allow, block, view and delete cookies of the mobile browser “Safari” that is developed by Apple. There is however no way for users to control the storage of, and access to, cookies by apps. Users can only delete cookies if the developer of an app has implemented that option, or by deleting the app.

An app dubbed Cookie Monster - developed for personal use by yours truly - to overcome this lack of control by iOS, shows that apps store cookies just like websites do.

\textsuperscript{181} Recital 65-66, Citizens’ Rights Directive.
\textsuperscript{182} An interesting side note is that native apps are confined to the development tools that are offered by the vendor of the mobile operating system. It would be unimaginable that websites would be confined to use development tools that are offered by vendors of browsers (setting compatibility issues aside).
\textsuperscript{183} The phrase ‘cookies’ also includes DOM-storage such as LocalStorage and Databases.
As there is no doubt about whether cookies that are placed by websites fall within the substantive scope of article 5 (3), it would be a great anomaly to have apps fall within the scope of the provision for the storage of and access to cookies, while denying its applicability for accessing other information that is peculiar to smart mobile devices.

When the e-Privacy Directive entered into force, and also when it was amended by the Citizens’ Rights Directive, it is likely that apps were not foreseen to fall within its scope. Irrespective of whether it was foreseen, the reality is that apps generally do access or store information on terminal equipment of users. They can also pose a threat to the privacy of users, when they access information without informing a user. Whether apps are malicious or not does not matter, the recitals of the Citizens’ Rights Directive explicitly recognize both legitimate and malicious purposes: the purpose of the access or storage of information is irrelevant.\(^{184}\) Apps can do exactly what the rationale behind the provision tries to protect users from: they can gain access to a lot of information without a user’s knowledge, store hidden information and track the behavior of users. Smart mobile devices are exactly the kind of equipment that have information that belongs to the private sphere of their users. Apps should - and do - therefore fall within the scope of article 5 (3).

The e-Privacy Directive does not contain any provisions regarding jurisdiction.\(^ {185}\) The territorial scope of the e-Privacy Directive is stated in article 3: “\textit{This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community, including public communications networks supporting data collection and identification devices}”. Debuserre states that this provision, in combination with the intention of the European legislature to regulate ‘electronic communication services in the Community’, also applies to information society services that are established outside the EU who offer their services to individuals within the EU.\(^ {186}\) The jurisdictional scope of the e-Privacy Directive however has to be determined according to article 4 of the Data Protection Directive, which acts as a lex generalis and has been discussed in the previous paragraph. Further analysis is required on a case-by-case basis whether

\(^{185}\) Kuner 2007, p. 135; Schnabel 2009, p. 84.
\(^{186}\) See article 1 (1) of the e-Privacy Directive; Debuserre 2005, p. 85; Kuner 2007, p. 138.
jurisdiction can be based on article 4 (1) (a) or 4 (1) (c) of the Data Protection Directive. What consequences the applicability of article 5 (3) has for publishers, will be discussed in the next chapter.

3.4 Conclusion
The evaluation of available data on smart mobile devices, demonstrates that a majority can be qualified as personal data under the Data Protection Directive. This is especially the case when different kinds of data, e.g. location data and UDIDs, are combined. As there is no standard set of data that apps utilize, a case by case analysis is required to determine whether personal data is processed. The results of monitoring the network traffic of several apps demonstrates however that personal data is widely processed by apps. Apps will therefore generally fall within the substantive scope of the Data Protection Directive (‘Directive’), with the exception of apps that do not process any personal data at all.

In most cases the publisher of an app is also the data controller, but there can be exceptions to this rule. Any actor that determines the purposes and means of the processing of personal data by or with apps will be a data controller. This may also include analytics and advertising companies. Regarding the jurisdiction of the Directive, a distinction can be made between data controllers of apps that are established within and outside of the EU. The former will generally be subject to the jurisdiction of the Directive based on article 4 (1) (a), as they are established within the EU. Further analysis on a case-by-case basis is required to determine which national law is (or national laws are) applicable in a specific case. As a significant amount of publishers are not established within the EU, it is paramount to determine whether they too fall within the jurisdiction of the Directive. When a publisher has no relevant establishment within the EU, article 4 (1) (c) can form the basis of jurisdiction if the publisher makes use of equipment that is located on Community territory for the processing of personal data. As smart mobile devices of users fall within the definition of “terminal equipment”, and publishers have control over what data is collected and for what purposes by means of their apps, the jurisdiction of the Directive can be based on article 4 (1) (c). When millions of European smart mobile device users use apps on Community territory of app publishers that are not established, or have
no relevant establishment, within the EU, the inapplicability of article 4 (1) (c) would create a severe lacuna in the protection of their personal data and the application of the Directive.

While article 5 (3) of the e-Privacy Directive is generally known for its applicability on cookies, apps also fall within its scope for two reasons. Firstly, apps can do exactly what the rationale behind the provision - information on terminal equipment of users belong to their private sphere and require protection under the European Convention on Human Rights - tries to protect users from: apps can gain access to information without a user’s knowledge, store hidden information and track the behavior of users. Secondly, apps access and store information on terminal equipment of users. While the recitals of the e-Privacy Directive mention that any information on the terminal equipment of users falls within their private sphere, a lot of personal data is available on smart mobile devices and are accessed by apps. As apps also store and access cookies, it would be a great anomaly to have apps fall within the scope of the provision for the storage of and access to cookies, while denying its applicability for accessing other information that is peculiar to smart mobile devices. Smart mobile devices are exactly the kind of terminal equipment that have information belonging to the private sphere of their users, and which the provision tries to protect. As a result apps fall within the scope of article 5 (3).
4. Analysis

"Apps must comply with all legal requirements in any location where they are made available to users. It is the developer's obligation to understand and conform to all local laws."

- Article 22.1 App Store Review Guidelines

This chapter analyzes the specific application of the Data Protection Directive (‘Directive’) and the e-Privacy Directive to apps and their publishers. The first section will focus on the Data Protection Directive and discuss five aspects of the Directive in the context of apps. These aspects consist of: the legitimate grounds, the proportionality principle, the legitimacy and purpose limitation principles and the transparency principle. For each aspect, following an introduction, its specific application to apps will be discussed. The researched apps in chapter two will be used to demonstrate, where possible, how each aspect applies to apps in practice. The second section will discuss article 5 (3) of the e-Privacy Directive and its interaction with the Data Protection Directive. The focus will be set on the obligation to inform users and to obtain their consent, while exceptions that are provided by article 5 (3) are evaluated as well. Where relevant, best practices for apps proposed by a variety of stakeholders, rules set by application catalog providers and recent developments on mobile privacy across the Atlantic will be discussed. Finally, recommendations that could increase transparency and user control on smart mobile devices will be made sporadically.

4.1 Data Protection Directive

Article 6 of the Directive contains principles relating to data quality. The fair and lawful processing of personal data, the first of the principles, could be regarded as the predominant principle. The fair processing of personal data implies that data subjects must be informed about who processes their personal data and for what purposes, while they are not deceived or

---

187 In this chapter the phrase ‘apps’ is interchangeable with ‘data controllers of apps’. As discussed in the previous chapter, this is often the publisher, but requires further analysis on a case-by-case basis. Where the phrase ‘publisher’ is used, it also denotes the developer of the application, as the developer is either the same person or entity as the publisher, or is under control of the publisher. The phrase developer is preferred over publisher when discussing technical aspects of apps.

188 Article 6 (1) (a) Data Protection Directive.
mislead.\textsuperscript{189} The lawful processing of personal data implies that the processing should be based on a legitimate ground, and should be in compliance with all legal requirements.\textsuperscript{190} In the following sub-paragraphs five aspects of the Directive will be discussed: the legitimate grounds for lawful processing, the proportionality principle, the legitimacy and purpose limitation principles and finally the transparency principle.

4.1.1 Legitimate grounds

The processing of personal data by a controller, can only legitimately take place if it is based on one or more of the six legitimate grounds that are set out in article 7 of the Directive. Depending on the circumstances, the processing could be simultaneously based on more than one legitimate ground.\textsuperscript{191} There are three relevant grounds on which apps could base the processing of personal data: the unambiguous consent of the data subject, the necessity for the performance of a contract to which the data subject is party, and the necessity for the purposes of a legitimate interest pursued by the controller.\textsuperscript{192} The remaining legitimate grounds in the Directive are irrelevant and fall outside the scope of this thesis, as apps generally do not have to process personal data to comply with legal obligations, do not have to protect the vital interests of data subjects, and do not carry out tasks in the public interest.\textsuperscript{193} In the following sub-paragraphs, the relevant legitimate grounds will be discussed in the order that they are found in the Directive. For each legitimate ground, following its introduction, an assessment will be made regarding its reconcilability with apps. The sub-paragraph on unambiguous consent will include recommendations in light of the challenges that apps present with regard to obtaining unambiguous consent from data subjects. Before discussing each legitimate ground, it is important to note that none of the legitimate grounds negate other obligations of controllers under the Data Protection Directive.\textsuperscript{194}

\footnotesize
\textsuperscript{189} Schnabel 2009, p. 562.
\textsuperscript{190} Kuner 2007, p. 90.
\textsuperscript{191} For an example see WP Opinion 15/2011, p. 8.
\textsuperscript{192} Articles 7 (a), (b) and (f) Data Protection Directive.
\textsuperscript{193} Article 7 (c), (d) and (e) Data Protection Directive. The necessity to process personal data to comply with legal obligations may be relevant for some apps, but falls outside the scope of this chapter.
\textsuperscript{194} WP Opinion 15/2011, p. 7;
4.1.1.1 Consent

A data controller may process personal data if data subjects have given their unambiguous consent. The Directive defines consent as “any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed”.\(^{195}\)

This paragraph will start with a description of the requirements for consent by data subjects, followed by an overview of recent developments in the United States regarding consent and apps. Subsequently an analysis will be made of how apps and mobile operating systems currently obtain consent from users, and whether that practice is reconcilable with the Data Protection Directive. Finally, a recommendation will be made about how mobile operating systems can aid users and apps in respectively giving and obtaining consent, that is reconcilable with the Data Protection Directive.

Several requirements can be found in the definition of consent. Firstly, consent must be given freely. This denotes that the data subject must be able to exercise a real choice.\(^{196}\) Secondly, consent has to be specific: the exact purpose of the processing must be explained by the controller.\(^{197}\) Finally, consent has to be informed. This is necessary to guarantee that individuals can make informed decisions about the processing of their personal data.\(^{198}\) Therefore data subjects must always have information about the processing, before there can be consent.\(^{199}\) This is inherently linked with the obligations of the controller under the transparency principle.\(^{200}\)

The Working Party is of the opinion that there are two additional requirements to ensure appropriate information. Firstly, the provided information should not be in legalese, but in plain text that is comprehensible by the average data subject. Controllers may not assume that their customers are technically skilled persons just because they own a smart mobile device.\(^{201}\)

\(^{195}\) Article 2 (h) Data Protection Directive.
\(^{196}\) WP Opinion 15/2011, p. 12.
\(^{197}\) Schnabel 2009, p. 543.
\(^{198}\) Schnabel 2009, p. 543.
\(^{199}\) WP Opinion 15/2011, p. 19.
\(^{200}\) Infra §4.1.4.
\(^{201}\) WP Opinion 13/2011, p. 18.
Secondly, the information should be given directly to data subjects. It is not sufficient if the information is made available somewhere.\textsuperscript{202}

The ‘unambiguous’ component of consent in article 7 (a) of the Directive, requires that there should be no doubt to the data subject’s intention to give consent.\textsuperscript{203} This relates to the manner in which consent is given or obtained. Consent can be given either expressly or implied. However, implied consent requires a cautious approach as there should be no doubt that the individual has given consent.\textsuperscript{204}

\textit{Recent developments on mobile privacy in the United States}

Before analyzing the implications of the legitimate ground of consent for apps, it is worthy to look at recent developments on mobile privacy across the Atlantic. Among catalog providers, Apple requires developers to obtain prior permission from users to process personal data.\textsuperscript{205} That there can be consequences for apps that do not inform their users about the processing of personal data, or do not obtain user consent, came to clear light in the course of writing this thesis.

In February 2012, Blogger Arun Thempi discovered and published that the social networking app Path (iOS) automatically uploaded his address book to the Path servers, without informing him or obtaining his prior permission.\textsuperscript{206} When the story got picked up by technology websites, it was soon discovered that Path was not the only app guilty of this practice: the Foursquare app operated in a similar way. Other apps (e.g. Twitter, Facebook and LinkedIn) uploaded address books of users when they tapped a ‘Find my Friends’ button, without making it clear to users that this would upload their address books.\textsuperscript{207} Morin, the CEO of Path, apologized to users in a blog post for the erroneous implementation of their ‘Find my Friends’ feature. Learning from their mistakes, Morin announced that the collected address book data of users was

\textsuperscript{202} WP Opinion 15/2011, p. 20.
\textsuperscript{203} WP Opinion 15/2011, p. 21; Schnabel 2009, p. 542.
\textsuperscript{204} WP Opinion 15/2011, p. 21.
\textsuperscript{205} Articles 4.1 and 17.1 App Store Review Guidelines.
\textsuperscript{206} Arun Thempi, ‘Path uploads your entire iPhone address book to its servers’, 8 February 2012, available at \texttt{http://mclov.in/2012/02/08/path-uploads-your-entire-address-book-to-their-servers.html}.
deleted, while also giving full disclosure of the purposes and use of the address book data. Morin furthermore explained that in a future update, the Path app would prompt users to opt-in for sharing their address books with Path.\textsuperscript{208} In an even later update, Path has laudably started to hash the address book data of users.\textsuperscript{209} Tom Neumayr, an Apple spokesman, commented on the issues with the iOS address book by stating that “apps that collect or transmit a user’s contact data without their prior permission are in violation of our guidelines”. He also explained that “[..] any app wishing to access contact data will require explicit user approval in a future software release”.\textsuperscript{210} Thus, in a future update of iOS, users will be prompted when an app tries to access their address book, similar to the standard pop-up of iOS when location data is requested by an app.

The Path debacle gave rise to debate on mobile privacy in the United States. Following the disclosure by Path, congressmen Waxman and Butterfield wrote a letter to Tim Cook, the CEO of Apple Inc., raising the question “whether Apple’s iOS app developer policies and practices may fall short when it comes to protecting the information of iPhone users and their contacts”.\textsuperscript{211} The congressmen send Apple a list of questions that they requested to be answered.

Apple’s answers to the questions of the congressmen make clear that Apple performs periodic random audits of apps for compliance.\textsuperscript{212} The letter furthermore states that “when Apple becomes aware of a potential violation, such as an app not obtaining consent prior to accessing user data in an address book, Apple investigates, contacts the application developer, and if necessary, works with the developer to remedy the violation. If an application developer refuses to come in to compliance, the application will be expeditiously removed from the App Store”.\textsuperscript{213}

Although Apple states that it conducts periodic random audits of apps, it seems to implicitly

\textsuperscript{208} Path, ‘We are sorry.’, 8 February 2012, available at <http://blog.path.com/post/17274932484/we-are-sorry?c8f39750>.
\textsuperscript{213} Idem.
agree that those audits are not foolproof, because Apple sees fit that users are prompted when their address books are trying to be accessed by an app. While this is a welcome step by Apple, it only covers the issue of address books; other data that will still be accessible by developers without obtaining prior permission from users, are left out. It is only a question of when and not if there will be similar misconducts by apps with other data that is readily accessible on iOS (e.g. calendars, and photos if prior permission for the use of location has been obtained).

In the end of February 2012, the Obama administration unveiled a proposal for a ‘Consumer Privacy Bill of Rights’.\(^{214}\) The Consumer Privacy Bill of Rights includes principles that are similar to those found in the Data Protection Directive: transparency, purpose limitation and proportionality. The Consumer Privacy Bill of Rights however is only a proposal at the moment, although the White House did call on Congress to pass legislation that would enforce the framework.

In March 2012, congressmen Waxman and Butterfield sent letters to 34 publishers of social apps on the App Store.\(^{215}\) The publishers were chosen because their apps were included within the ‘Social Networking’ category of the ‘iPhone Essentials’ subcategory in the App Store. Among the apps concerned are for example Facebook, Twitter, Foursquare, Instagram and Path. The letters included nine questions that would form the basis for the congressmen towards “building a fact-based understanding of the privacy and security practices in the app marketplace”.\(^{216}\) The questions concerned, inter alia, the availability of privacy policies, obtaining user consent, and the use of address books, UDIDs and MAC-addresses.\(^{217}\) The responses of the publishers are unfortunately not publicly available, which bars their evaluation. The letters sent by the congressmen however does show that that application catalogs and apps are under close scrutiny by officials in the United States.

---


\(^{216}\) Idem.

The mobile privacy debate is gaining momentum in the United States. It will be even more interesting to see what effects the debate in the United States will have on mobile privacy, as mobile operating systems, application catalogs and publishers of apps are under close scrutiny by the United States Congress, the Federal Trade Commission and the Attorney General of California. In Europe, mobile privacy is slowly but surely gaining attention. The opinion of the Article 29 Working Party on geolocation services on smart mobile devices demonstrates that there is no lack of attention for mobile privacy. Although the intensity of the attention may be lower in Europe, more scrutiny can be expected in the future as the Article 29 Working Party and the French Data Protection Authority (‘La Commission nationale de l’informatique et des libertés’) have stated to include mobile privacy in their working programs for 2012. Scrutiny by regulatory and political bodies on both sides of the Atlantic is laudable, as their goals presumably coincide and could have a positive effect on the mobile privacy of users.

**Unambiguous consent and apps**

An interesting question is how apps could obtain unambiguous consent. Can the mere installation of apps by users be considered as unambiguous consent? When users are not presented with specific information before or during the first use of an app, the answer is likely to be negative. Without information, users can not indicate their specific and informed wishes: one simply can not consent to something one has no idea of. Apps might however be able to obtain unambiguous consent if users are provided with a privacy policy before, upon the first use of an app, or when apps actively require consent from users by pop-ups.

While there currently is no designated area in application catalogs for providing users with privacy policies of apps, it will be an option in the near future. Publishers can use that opportunity to include privacy policies on the description page of their app so that users can decide beforehand whether to install and use an app. This does not guarantee however that users are informed, or consent to the processing of their personal data. They might simply not be aware

---

218 Infra §4.1.4.
219 Supra note 5.
220 Infra §4.1.4.
Therefore the privacy policy should also be available within the app. It is the most logical place where users expect to be able to find a privacy policy. To inform users, apps should display their privacy policies to them upon the first use of the app. It is important that the privacy policy is clear and comprehensible. The relatively small screen estate on smartphones (as opposed to tablets generally have a larger screen) can present challenges in this regard.

Presenting a privacy policy upon the first use of an app does not disturb the usability of the app, as the process will only have to take place once: consent will generally be valid unless for example the purpose of the processing of data changes or when data subjects withdraw their consent. It is important to note that if the purposes of processing do happen to change - and the app is for example updated - consent will have to be obtained again from users. But even displaying a privacy policy may not satisfy the requirements of consent if users just click through and accept the privacy policy. While one can argue that this is a clear indication that data subjects have a lack of concern for their privacy, this argument can be countered with the fact that apps need to do a better job at informing and obtaining consent from data subjects, if they want to base their processing of personal data on unambiguous consent.

As was demonstrated in chapter two, there is a practice in mobile operating systems that gives users control - to some degree - of the information that apps can access. This is achieved by either presenting pop-ups to users when data is actually trying to be accessed (e.g. location data on iOS), or by displaying a list of data that an app requests access to upon installation (the majority of data on Android). Levis notes that “permissions are important because a user-defined permission is evidence that a user consents to the application accessing that data”. There is no doubt that in both options users have to take affirmative action to give apps permission to access such data. The affirmative action to access data however, can not simply be qualified as consent to the processing of data, if the purposes of the use of data are unknown. Consent can not be obtained via pop-ups or permission models of mobile operating systems.

---


222 This practice is recommended in the Electronic Frontier Foundation’s Mobile User Privacy Bill of Rights, and the GSM Association’s Mobile Privacy Design Guidelines.

unless those pop-ups and the privacy policies of apps supply users with information about how and why their data is processed.

The iOS location data pop-up has an option for developers to present the user with information about the purpose of the processing of location data, but it is rarely used by apps. While Apple requires apps to obtain prior permission of users and provide them with information on how and where the data will be used, the purpose specification in the location services API is not obliged.  

Similarly Android allows developers to request access to data, but does not provide a way to specify how the data will be used and for what purposes, when the permission list is presented to users. Users therefore have no way of knowing how an app will use the requested permission to access their call logs for example. While the practice by mobile operating systems of giving users more control as to what data apps can access is laudable, it is inherently flawed if apps do not have to specify how and why the data is processed.

Only when the use of data is covered in a separate privacy policy, or when such pop-ups or permission lists include information as to what the purpose of the processing is, and how the information is going to be used, could it be deemed as unambiguous consent. This leads to the conclusion that the current model of pop-ups or permission lists are not adequate to obtain the unambiguous consent of users.

Recommendations

A more coherent way of dealing with unambiguous consent of users, from the point of view of the mobile operating system, would be a hybrid solution between the iOS pop-up dialogs and the Android permission list. Unlike the current situation though, developers would be obliged to specify the purposes and use of data.  

Envisioning this could result in the following practice.

---

224 Articles 4.1 and 17.1 App Store Review Guidelines.
225 FTC 2012-1, p. 10.
Publishers can implement a privacy policy that can be viewed by users before installing an app. Before or during the installation process of the app, or ultimately upon the first use of the app, users are presented with a permission list of data that an app tries to access to. This list includes data that is unconditionally required by an app to work properly. Optional data on the other hand is handled via pop-ups. If there is a need for data that are not essential to the app, but are rather needed for optional services that a user might want to use (e.g. a find my friends feature or location data), consent could be obtained by displaying a pop-up when the data is actually needed by the app. This pop-up would once again be required to inform users about the purposes and use of the data. Users should furthermore at all times be able to withdraw their consent, and be able to view the permissions they have given to an app. A congregate permission list for essential data provides advantages for the usability factor of apps, as otherwise users would be presented with an overload of pop-ups.

The permissions list should be easy to comprehend and include the purposes of the processing, and how the requested data is used for each distinct item (e.g. location data, photos, messages). It should also include the privacy policy of an app, that can have additional information about the processing of data. If a user chooses not to consent to the permission list, the app will fail to install or function.

A hybrid solution to permission lists and pop-up dialogs gives users more control over their data, and forces developers to think about data minimization. While there are no technical limitations to already implement portions of the above mentioned system by developers of apps, it is ultimately up to the developers of the mobile operating systems to design and implement such a system. If the above mentioned model of pop-ups and permission lists is implemented on the level of the mobile operating system, developers have to adhere to the system.
4.1.1.2 Contract

Article 7 (b) of the Data Protection Directive states that where a contract exists between a data subject and a controller, the latter may process personal data if it is necessary for the performance of that contract. This legitimate ground first of all begs the question whether a contract exists between the publisher of an app and the user.

The End User License Agreement (‘EULA’) of apps could form a contract between a publisher and a user. As was discussed in §1.6, publishers are not obliged to implement an EULA. If the publisher does not implement an EULA, the app is either covered by a standard EULA drafted by the operator of the application catalog, or is contractually obliged by the operator of an application catalog to give users a standard non-exclusive, worldwide and perpetual license to use their app. If the publisher does implement an EULA however, it overrides the standard license of use. Four scenario’s can be distinguished from §1.6 regarding EULAs and their implementations in apps and application catalogs.

(1) There is no EULA provided by an app, it is governed by a standard license.
(2) There is an EULA provided by an app. The EULA is embedded, or linked to in the product description page but it is not available within the app. Users have an option to view the EULA before installing the app.
(3) There is an EULA provided by an app. It is only available within the app. A user has to install the app before it can view the EULA. The EULA is either presented to users upon installation, or users can view the EULA on their initiative.
(4) There is an EULA provided by an app. The EULA is embedded or linked to in the product description and it is available within the app. Users have an option to view the EULA before and after installing the app. The EULA might be presented to users upon installation.

The basic assumption of article 7 (b), is that a valid contract must exist between the data subject and the controller. Only if the contract is valid, can it form the basis for the processing of personal data that is necessary for the performance of that contract. It is safe to presume that - no

matter what the applicable law is - a certain form of consent or assent will be required to constitute a valid contract. This ‘consent’ however, does not necessarily have the same meaning as consent in the sense of article 7 (a) of the Directive. The latter is the expression of the agreement of a data subject to the processing of his personal data, and has a different purpose than ‘consent’ regarding the constitution of contracts. The Directive does not assess the validity of a contract; it is a presumed fact, for which the data controller bears responsibility.

To limit the scope of the thesis, it is assumed that the EULAs in the above mentioned scenarios are valid contracts between publishers of apps and users. While the validity of the contracts is henceforth assumed, it is by no definition a given that the EULAs are indeed valid contracts.228 Especially since users - as the differences between scenarios two, three and four demonstrate - can not easily view and consent to EULAs. Although developers have the technical ability to present EULAs to users within apps in order to obtain their consent, only a small fraction does so.229

The standard licenses in the first scenario are inherently generic, do not contain any information about the specific services provided by an app and do not cover the processing of personal data.230 They can therefore not form the basis for the legitimate ground of contract, as the processing of personal data is not necessary for the performance of the EULA. The Working Party notes that the assumption that users would enter in to a de facto contractual relationship when using the services of a website, does not meet the strict limitation of necessity as required by the legal ground of contract.231 There is no reason why this would be any different for services provided by apps. Additionally, even if a standard licensed app has a privacy policy, that does not change the fact that any processing of personal data can not be based on the legitimate ground of contract.

In the other scenarios, the app has provided its own EULA. It will depend on the services provided by an app and the contents of a specific EULA, whether the processing of personal data is necessary for its performance. EULAs generally establish the rights and obligations of the

---

228 Good et al. 2006, p. 289.
229 Of the tested apps in chapter two, only Dosecast presented an EULA.
licensor and the licensee. They are often long documents in legalese that are not easily comprehensible by users, and are presented to users as ‘click-through agreements’.\textsuperscript{232} Despite these hurdles, if one is to assume that EULAs are valid contracts, it can be concluded that EULAs could form the basis for the processing of personal data. It has to be noted however that, as a majority of apps do not provide their own EULAs, their processing of personal data can not be based on the legitimate ground of contract.

4.1.1.3 Legitimate Interest

The final legal ground on which apps could base the processing of personal data, is the ground of legitimate interest. It can form the basis for the processing of personal data when the “processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1)”\textsuperscript{233}

The legitimate interest ground balances the legitimate interests of the controller with the interests for the fundamental rights and freedoms of the data subject. Only when the latter does not override the legitimate interests of the controller, can the ground of legitimate interest form the basis for the processing. Because of the balancing nature of the provision, cautiousness is necessary on a case-by-case basis.

Whether the legitimate interest pursued by an app can legitimate its processing of personal data, will naturally depend on the interests that are pursued by it. Factors that can play a role in the balancing process are the sensitivity of the data and the safeguards that are implemented by the controller.\textsuperscript{234} As smart mobile devices are highly personal devices that have a lot of personal data stored on them, and users generally do not have a lot of control over their data, it is difficult to imagine that the interests of data subjects do not override the pursued interests of controllers. The fact that information that is stored on smart mobile devices of users are considered to be part of their private sphere, and which requires protection under the

\textsuperscript{232} Good et. al. 2006, p. 289.
\textsuperscript{233} Article 7 (f) Data Protection Directive.
\textsuperscript{234} Hooghiemstra & Nouwt 2007, p. 68.
European Convention for the Protection of Human Rights and Fundamental Freedoms, furthermore denotes that the interests of users weigh heavily.\footnote{Supra note 174.}

The nature of the legitimate interests pursued by apps can differ greatly, and are hard to discuss \textit{in abstracto}. They will therefore not be discussed in this paragraph. However, whatever the pursued interest of an app may be, the processing of personal data is dependent on whether the data is \textit{necessary} for those interests. A controller will therefore, even if there is a legitimate interest that outweighs the interest of data subjects, only process data that is necessary for the purposes of the pursued interests.

When the processing of personal data is based on the legitimate interests of the controller, data subjects have the right to object to the processing.\footnote{Article 14 (a) Data Protection Directive; Schnabel 2009, p. 563.} For a justified objection, data subjects have to provide compelling legitimate grounds relating to their particular situation. When there is a justified objection, the controller may no longer process the data of the data subject.

While in some cases the legitimate interest of an app may justify the processing of personal data, controllers should wonder whether it is the appropriate legitimate ground depending on what data is processed. In the interest of transparency and certainty, and to fortify the trust of users in an app, unambiguous consent could be a more appropriate legitimate ground. It is interesting in this regard to note that the Working Party is of the opinion that for the processing of location data in the context of information society services, the main applicable legitimate ground is prior informed consent due to the sensitivity of the data.\footnote{WP Opinion 13/2011, p. 14.} It is however not clear what this position of the Working Party is based on, as there is no extensive motivation behind it. Given that the argument is grounded on the \textit{sensitivity} of the data, it is possible that the position of the Working Party is not based on article 5 (3) of the e-Privacy Directive - although that can not be ruled out - as the sensitivity of the data does not play a role in that provision. Given that the Working Party requires prior informed consent, it seems furthermore that the argument is not based on the Data Protection Directive either, as prior informed consent is not a legitimate ground in the Directive. The lack of motivation behind the reasoning makes it hard to judge the opinion of the Working party. Despite that, it is clear that the the Working Party is of...
the opinion that the processing of location data can not be based on other ‘legitimate grounds’ than prior informed consent.

Apps and advertising companies, presumably, often base their processing of personal data on the ground of legitimate interest, when they do not - or choose not to - obtain unambiguous consent from data subjects.\(^{238}\) It is however questionable whether their interests are not overridden by the interests of data subjects. Sloot and Borgesius argue that the interests of data subjects should probably prevail in the context of behavioral advertising, because “the tracking of online behaviour can paint a highly detailed picture of an Internet user, which is often regarded as an invasion of privacy”.\(^{239}\) This argument is even stronger in the context of apps, as apps and mobile advertising companies can not only track the behavior of users, but can possibly gain additional information, such as location data, because of the capabilities of smart mobile devices. It can however not be ruled out that in a specific situation, depending on what data is processed and for what purposes, the interests of a controller could be more important than the interests of data subjects.

4.1.2 Proportionality

The proportionality principle requires that personal data needs to be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.\(^{240}\) This principle is often referred to as ‘data minimization’, although it is not explicitly mentioned in the Directive.\(^{241}\) Schnabel states that data minimization should be understood as an appeal for using technical possibilities to minimize the need for the processing of personal data.\(^{242}\) It follows from the the proportionality principle, that apps must only process data that is relevant and not excessive for the purposes for which they are collected. But as the results discussed in chapter two can demonstrate, excessive or irrelevant collection of information is easily achieved by apps. The following paragraphs discuss the irrelevant and excessive collection of data by apps.

\(^{238}\) Other legitimate grounds are presumed to be irrelevant as it is unlikely that mobile advertising companies can base their processing of personal data on other legitimate grounds besides unambiguous consent and legitimate interest.

\(^{239}\) Sloot & Borgesius 2012, p. 99.

\(^{240}\) Article 6 (1) (c) Data Protection Directive.

\(^{241}\) Kuner 2007, p. 73; Schnabel 2009, p. 561.

\(^{242}\) Schnabel 2009, p. 561.
apps, and demonstrate how data minimization can play a role in preventing the irrelevant and excessive collection of data. A look will also be taken at what rules operators of application catalogs have set regarding the proportionality of collected data by apps.

The NU app collects location data of users and the UDIDs of their devices. Although its privacy policy does not mention the purpose or use of UDIDs and location data, it can be inferred from using the app that location data is used to display local weather information, while the UDID is processed to track users. The location data and UDIDs of users are transmitted to an advertisement company, presumably for the purposes of targeted advertising. Based on their exact location, users are placed in one of the six available regions in the Netherlands for weather information. Users can however also manually select the region for which they wish to display weather information. One could argue that the use of location data is excessive for the NU app, as users could and can also manually select one of the six available regions. But even assuming that the use of location data is necessary and not excessive, for arguments sake, retrieving the exact location of the user is excessive. The location data API in the iOS SDK offers developers granular control over the accuracy of the location data. They are able to choose between five levels of accuracy: ‘best’ accuracy, accurate to within the nearest ten or hundred meters, and accurate to the nearest one or three kilometers. In the case of the NU app, the least accurate level of location data would be sufficient to place a user in one of the six regions. Using location services may not always be relevant or a necessity for the provided services. Even if it is deemed necessary, one should question whether obtaining the exact location of a user is really necessary, or whether a less accurate location is sufficient.

The game Little Lost Chick implements and uses the social gaming platform Crystal. Crystal collects UDIDs, location data, address books (first and last names, e-mail addresses) in case a user tries to find friends, e-mail addresses, GameCenter IDs, and if users chooses to connect to Facebook, the Facebook IDs of users. One could wonder why a game would need to collect all this information. Crystal’s privacy policy (only available in-app) enumerates a list of information they collect. This list includes all the above mentioned data, save for the address

---

243 It has to be noted that when developers do not specify a level of accuracy, the default accuracy is automatically set to ‘best accuracy’ by the iOS SDK. It would be a welcome change if Apple requires developers to specify the level of accuracy, instead of settings the default accuracy to ‘best’, or to set the default accuracy to the least accurate possibility.
books and Facebook IDs. The purpose for collecting the information is stated as ‘to improve products and services’ and for ‘market research’. The purposes are not very illuminating, let alone specified or explicit. The exact purpose of the use of location information is unknown as it is not specified by the app, nor is there any clear geolocation service provided by the app. When users choose to use the ‘find my friends’ feature of the app, the address book information, or Facebook profile of the user, is used to find friends. The app features a button labeled ‘Find friends via contacts’, that has the following subtitle: “Automatically match friends from email addresses in your local [sic]”. When the button is pressed, a pop-up is shown where the user is explained that his address book is temporarily shared with Crystal to match existing Crystal users, and that the information is not retained. The user is then asked for permission to transmit the address book to Crystal’s servers. Why the use of the address book is not covered in Crystal’s privacy policy, is unknown. Looking at the find my friends feature of Crystal, or any other app that uses a similar feature and uses multiple identifiers, one can argue that the collection of data is be excessive for two reasons: first, to match users one could suffice with the use only one identifier, for example an e-mail address, depending on how the app chooses to match users. Any additional identifiers like the first and last names or phone numbers do not need to be collected, unless there is an additional justifiable need for comparing more than one identifier to achieve greater accuracy. One identifier, chosen by the publisher, can be sufficient. Second, even when one or multiple identifiers are used, one does not actually have to process the address book in an identifiable form. Developers have proposed a more privacy friendly implementation of the find my friends feature, by using hashing.\footnote{Martin May, ‘PathGate and Best Practices for Implementing “Find Friends”’, 8 February 2012, available at \texttt{<http://blog.forkly.com/2012/02/pathgate-and-best-practices-for-implementing-find-friends/>}.} Hashing is explained as “the result of a one-way function that takes some input […] and spits out something that looks like this: 2fd4e1c67a2d28fc ed849ee1 bb76e739 1b93eb12”.\footnote{Idem.} The e-mail address used in chapter two would result in the following hash (if calculated with the MD5 algorithm): bbe8697c 4d9d292417f9178f 8161e184. By hashing the address book locally on a SMD, only the hashed identifiers
are uploaded to the servers of the app, in a form that does not directly identify individuals.  The hashed identifiers are then used to match the hashed identifiers of users that already have an account on the service. When the hashes match, the friend can still be connected, as if the identifier was transmitted without hashing. Afterwards the hashed identifiers that did not lead to any results, can be deleted as they can be deemed obsolete. A find my friends feature can therefore be implemented without actually transmitting address book data of users.

The proportionality principle is also found in the iOS Developer Program License Agreement, which forms an agreement between Apple and publishers of apps on the App Store. The agreement states that “You and Your Applications may not collect user or device data without prior user consent, and then only to provide a service or function that is directly relevant to the use of the Application, or to serve advertising”. The same article in the agreement also contains the following prohibition: “You may not use analytics software in Your Application to collect and send device data to a third party”. Seeing that most apps in the App Store use analytics software, the enforcement of the rule by Apple is questionable. The proportionality principle of the Developer Program License Agreement is further elaborated on in the App Store Review Guidelines. Developers are only allowed to use location data when it is directly relevant to the features and services provided by the app, or to support ‘approved’ advertising uses. In short, publishers are not allowed to collect location data if their app does not necessarily need them. The phrase ‘or to support approved advertising uses’ seems to indicate the use of Apple’s iAd advertisement platform, which is known to use location data. Whether the mere collecting of location data by apps for third-party advertisers is allowed, is unknown. There are however many ways to implement location data in a trivial way within apps, to make them seem relevant and legitimate.

Apple furthermore prohibits apps “that require users to share personal information, such as e-mail address and date of birth, in order to function”. While to the letter the rule seems

246 Other developers have argued that only hashing is not enough for anonymity, instead a technique called salting, where an additional string only known to the controller is appended to the input information before the hashing process takes place, should be used. See M. Pearce et al., ‘Pass the iOS Privacy Salt – Hashing Does NOT Guarantee Privacy’, 15 February 2012, available at <https://securitydreamer.wordpress.com/2012/02/15/pass-the-ios-privacy-salt-hashing-does-not-guarantee-privacy/>.
247 Article 3.3.9 iOS Developer Program License Agreement.
248 Article 4.4 App Store Review Guidelines.
249 Article 17.2 App Store Review Guidelines.
strict, there are lots of apps in the App Store that actually require users to sign up for an account, notably social media apps, in order to function correctly. The rationale behind the rule could be to prohibit rogue and malicious apps from collecting personal data in order to function, while the personal data is actually not needed for the functioning of the app. The thresholds put by Apple are welcome, but they stand or fall with their enforcement by Apple.

As a lot of data can easily be obtained from smart mobile devices, app publishers and developers need to ask themselves the question whether they actually need the data they collect, and for what purposes. With the vast amount of data available, excessive collecting of data is easy, although it may not always be necessary for the purposes for which they are collected.

### 4.1.3 Legitimacy and purpose limitation

A prominent principle of data quality is the legitimacy and purpose limitation principle: data must be collected for specified, explicit and legitimate purposes, and not further processed in a way that is incompatible with those purposes.\(^{250}\) The principle has two components. First, apps must only collect data for specific, explicit and legitimate purposes. Second, apps can not process collected data for further purposes that are incompatible with the original purpose.\(^{251}\) Universal or vague purposes do not meet the demands of the purpose limitation principle.\(^{252}\)

Illustrating this principle with practical uses by apps can shed more light on its implications for apps: consider an app that collects the address book of users, to notify them of their contacts that use that app too. This process is commonly referred to as the ‘find my friends’ feature. The app is able to find friends of a user by collecting and matching address book data (e.g. either a combination of identifiers like names, phone numbers and e-mail addresses or a single identifier). This can be a legitimate purpose to collect the data, when it is properly specified and explicit. When the address book is solely collected for the purpose of finding a user’s friends however, the address book can not be further processed for other purposes that are incompatible with the purposes that the data was originally collected for. Further processing of data is only allowed when it is compatible with the original purpose. A publisher therefore may

---

250 Article 6 (1) (b) Data Protection Directive.
251 Kuner 2007, p. 100.
not use the collected data from the address book with the original purpose of a find my friends feature, to send invitations to contacts of the user that do not use the app, or transmit it to third parties like analytics or advertising companies, as those purposes can hardly be deemed to be compatible with the original purpose of finding a user’s friends. This is also true for any other information, like location data. When location data is solely collected for the purpose of providing a geolocation service, it can not subsequently also be used for targeted advertising as that is incompatible with the original purpose. That apps do not always adhere to the purpose limitation principle can be demonstrated with the NU app, as discussed in §4.1.2. The NU App collects location data of users to present them with local weather forecasts. NU however also transmits the collected location data to an advertisement company. Although NU does specify the purposes for which the location data is collected, it is clear that the above mentioned purposes are incompatible. It can be concluded that apps need to clearly stipulate the purposes for which they collect data, and may not further process data for purposes that are incompatible with the original purpose that the data was collected for.

As developers and publishers - for various reasons - do not always have the privacy of their users in mind, various parties have drafted best practices or guidelines for mobile apps to respect the privacy of users. 253 The Electronic Frontier Foundation’s ‘Mobile User Privacy Bill of Rights’ informs publishers about ‘focused data collection’ and ‘respect for context’. 254 These principles match with the rationales of the proportionality and purpose limitation principles of the Directive. Furthermore, the GSM Association (‘GSMA’) released its ‘Privacy Design Guidelines for Mobile Application Development’ in February 2012. 255 The GSMA announced that mobile operators in Europe will implement the guidelines in their branded apps, while they invite other parties to follow their example. The purpose of the guidelines is to create a harmonized approach to user privacy across mobile platforms, with a consistent functional

treatment of their privacy and innovation in the development of privacy controls. The guidelines contain best practices that are clearly stipulated in plain language and include practical examples. Therefore it does not bar publishers or developers from comprehending the guidelines. Privacy by design is a keyword in the GSMA’s guidelines. The purpose limitation and proportionality principles can be found in the guidelines under “minimise information you collect and limit its use” and “do not surreptitiously access or collect personal information”. These initiatives are a good source of information for publishers and developers to design apps that respect user privacy.

4.1.4 Transparency

Another fundamental principle of the Data Protection Directive, is the obligation to inform data subjects about the processing of their data. When controllers process information of data subjects, they are obliged to provide them with information about the processing. This information has to include, at a minimum, the identity of the controller and the purposes of the processing for which the data are intended. Where necessary to guarantee fair processing, and depending on the specific circumstances in which the data are collected, additional information has to be provided as well. Additional information can for example be the recipients or categories of recipients of the data, and the existence of the right of access and/or the right to rectification. Users are often informed about the processing of their data by the privacy policy of a controller.

Although application catalog providers require apps to implement privacy policies (or other statements) regarding the processing of personal data, apps do not always adhere to that requirement. A study by the Wall Street Journal concluded that 45 of the 101 tested apps on

259 Article 10 (a) and (b) Data Protection Directive; Schnabel 2009, p. 562.
the Android Market and the App Store did not provide privacy policies on their websites, or inside the app.262 A similar study performed by the Future of Privacy Forum showed that 22 out of the 30 ‘top 10’ downloaded apps across the Android Market, App Store and Blackberry World, lacked a privacy policy.263 The Federal Trade Commission drew similar conclusions in a specific study on apps related to children.264

The processing of personal data by apps is often not transparent to users for three (non-cumulative) reasons: (1) apps are not informing users about the processing of their personal data, (2) apps either inform users incorrectly or incompletely, and (3) there is no ‘designated area’ in application catalogs and within apps to inform users. In this paragraph, the first two reasons will be discussed together in light of the transparency principle, followed by the third reason. Where possible, the lack of transparency is demonstrated with the apps that have been researched in chapter two. Finally, the focus will shift towards current developments in the United States that are related to the transparency of apps.

Some apps simply do not inform users about the data they collect and do not implement a privacy policy. This practice can for example be seen in the NU and Little Lost Chick apps, as discussed in §2.5, which lack a privacy policy within their apps. Where there is a privacy policy available, it may be incorrect, or not clearly inform users about what data is exactly collected, for what purposes the data is used, or with whom it is shared.265 This is for example the case in the Dosecast, TVGiDS.TV (Lite) and Instagram apps. The Dosecast app asserts that it does not process personal data, while it does in fact process the UDID of users alongside their medical information. Similarly, the privacy policy of the TVGiDS.TV Lite app mentions that no personal data is processed, although the app processes UDIDs of users. The TVGiDS.TV (not to be confused with the ‘Lite’ version) mentions several specific uses of the UDID. It however does not mention that the UDID is shared with third parties, as can be seen in the results displayed in figure A.2. The privacy policy of Instagram is - curiously - targeted as if Instagram was a website.

---

262 Supra note 3.
263 Applicationprivacy.org, ‘FPF Find Nearly Three-Quarters of Most Downloaded Mobile Apps Lack A Privacy Policy’, 26 May 2011, available at: <http://www.applicationprivacy.org/?p=723>. NB: Four apps did have privacy policies, but they were not accessible within the application.
265 See for example the apps Dosecast and TVGiDS.TV Lite that claim in their privacy policy to not process personal data, while they are processing the UDID.
instead of an app. The privacy policy mentions that Instagram collects ‘non-personally-identifying’ information for website statistics, and ‘potentially personally-identifying information’ like IP-addresses and user comments. It furthermore states that Instagram collects ‘personally-identifying information’ in the form of usernames and e-mail addresses from users that sign up for an Instagram account, including optional user-entered data such as first and last names. No mention is made however of what data the Instagram app processes besides the username and e-mail address. Users are for example not informed about the processing of UDIDs, location data, Twitter IDs or address books. This lack of transparency can be troublesome for users, and was recently demonstrated by raised user concerns on the acquisition of Instagram by Facebook.\footnote{CNET, ‘Facebook-Instagram deal raises new privacy worries’, 9 April 2012, available at <http://news.cnet.com/8301-31921_3-57411530-281/facebook-instagram-deal-raises-new-privacy-worries/>}  

The third reason that can explain the lack of transparency of apps, is the lack of a designated area to inform users. Even if there is a privacy policy in place that adequately informs users, there is no designated place within apps or the application catalogs where users can easily retrieve a privacy policy. Apps do not have a standard manner of implementing privacy policies. While on websites a privacy policy is usually retrievable with a link in the footer of a page or elsewhere, there is no designated or logical way of presenting privacy policies to users of apps.  

Privacy policies of apps can be implemented on two levels: within apps, and in application catalogs. On the first level, the privacy policy is implemented inside apps. This can either be in full text or by providing a link to the privacy policy on a website. It is either displayed to users before the first use of the app in the form of a pop-up or splash screen, or can be found elsewhere within the app. Depending on the design of the app, it is generally found in the ‘settings’ page, or beneath several levels of options. The consequence of this practice is that users often have no information about what data an app processes before they actually use the app. Users can only find out what data is being processed after using an app, and often after their data has already been processed.\footnote{During the research of apps in chapter two, it was frequently seen that apps already process personal data upon the first launch of the application.} On the second level, the privacy policy is implemented in application catalogs. As was discussed in §1.6, application catalogs do not provide a designated
area for publishers to provide users with their privacy policies.\(^{268}\) The only way publishers can provide users with their privacy policy \textit{before} installing an app, is by providing a link to their privacy policy in the description of the app.\(^{269}\)

The lack of transparency of apps has been addressed by senator Franken of the U.S. Congress in May 2011.\(^{270}\) In a letter to Steve Jobs and Larry Page, respectively former CEO of Apple Inc. and current CEO of Google Inc., senator Franken petitioned them to require apps to have privacy policies. The efforts of the senator did not yield any visible results. In February 2012, the attorney general of the state of California, Kamala Harris, reached an agreement with six leading operators of application catalogs to improve the privacy of users.\(^{271}\) This agreement is the outcome of the goal of the attorney general to enforce California’s “Online Privacy Protection Act” on mobile platforms.\(^{272}\) The agreement concerns the following application catalogs: Amazon’s App Store for Android, Apple’s App Store, Google’s Android Market, Hewlett-Packard’s App Catalog, Microsoft’s Windows Phone Marketplace and Research In Motions’ BlackBerry App World. The agreement contains provisions that oblige apps that process personal data to post a privacy policy (or other statement) that provides clear and complete information about how personal data is collected, used and shared by the app. It was furthermore agreed upon that the application catalog providers will implement designated areas in their application catalogs to provide users either with the full text of privacy policies, or a link thereto. This process shall be made available to publishers during the app submission process, and is optional.\(^{273}\) Additionally, the catalog providers will implement means for users to report apps that do not comply with applicable terms of service and/or laws. Finally, the participants to

\(^{268}\) The App Store does have a designated area for EULAs of apps, which could include a privacy policy.


\(^{273}\) One could argue that if apps that process personal data are required to implement a privacy policy, this option should not be tentative, as apps that do not implement privacy policies can be regarded as not processing personal data.
the agreement have agreed that an evaluation of privacy in the mobile space will take place within six months.

This is a laudable step of the attorney general, and catalog providers alike. While most catalog providers already require developers to provide privacy policies, publishers do not always adhere to those rules, nor do catalog providers actively enforce them.274 Catalog providers do not have an obligation to enforce, *inter alia*, the transparency principle of the Directive on publishers, as the transparency principle is only applicable to data controllers or their representatives.275 The transparency obligations of data controllers of apps that process personal data, stem directly from the Data Protection Directive and are applicable irrespective of any rules set by catalog providers. Catalog providers however have deliberately chosen to set rules regarding the transparency of apps, in spite of the direct obligations of publishers under the Data Protection Directive. These rules are part of the contractual relationship between catalog providers and publishers. The enforcement of the rules are therefore at the discretion of the catalog providers. The existence of these rules are commendable as catalog providers are gatekeepers of application catalogs. The lack of enforcement of these rules by catalog providers however is worrying: they have autonomously decided to set their own rules regarding the requirement of privacy policies and are the principle party that has the power to directly influence publisher behavior, at the high cost of prohibiting the publication of apps. The fact that enforcement is lacking can have several causes. A root cause might be the fact that auditing whether apps need to implement, or correctly implement, privacy policies is practically impossible for catalog operators, especially with the great amount of apps available. This would also mean that there would have to be an ex-ante review process like Apple currently operates. Even so, a designated area in the application catalogs for privacy policies can better inform users - if of course, there is a privacy policy. Google has been the first party to implement a designated area for privacy policies in its catalog per the agreement.276 To what extent the option of users to report apps that do not comply with applicable laws will make catalog providers take action, is

---

274 Whether the transparency rules set by catalog providers are reconcilable with the transparency principle of the Data Protection Directive, falls outside the scope of this paragraph.

275 Article 10 Data Protection Directive.

yet to be seen. Transparency alone is no guarantee for fair processing, as Wetherall et. al. discuss: “A privacy policy may be reassuring when read, but there is no guarantee that it is an accurate reflection of what happens in practice due to oversights, changes over time, and deception. Similarly, a mobile app may be configured to use encryption or expected to protect privacy, but there is no independent check for correctness.” It is however an essential step towards fair processing.

It can be concluded from the transparency principle, that apps have to inform users about what data they collect and for what purposes the data are used. Considering that apps can access intricate information on smart mobile devices, sometimes even without knowledge of their users, they should comprehensively inform users about all data they process, in order to guarantee fair processing. No data that is processed should be omitted, nor with whom the collected data is shared. This is especially significant for apps that use analytics and advertisement provided by third parties. Although it may not be clear what data these third parties collect, as the developer of the app often merely incorporates a SDK, it is the publishers responsibility to inform users about what data is collected by analytics and advertising companies. In this regard, it does not matter whether the publisher of the app acts as a data controller or not. It is notable that in the United States several law suits are pending over the surreptitious transmission of UDIDs by apps to third parties.

Furthermore, users should be provided with a clear description of the purposes for which their data are intended to be processed. When an app collects a significant amount of information and merely mentions that the purpose of the collection is for ‘market research’, users are not adequately informed; users will not know what the market research entails or how their data is relevant for that purpose. Attention therefore needs to be given to the clear stipulation of purposes for which the data is processed, so users can be adequately informed. In this regard, the

---

277 Wetherall et. al. 2011, p. 2.
278 In this regard see the disclosure of the use of cookies by websites. See WP Opinion 1/2008, p. 22.
279 Generally, information collected by analytics and advertising companies can be found in their privacy policies. Developers should however independently find out what data is actually collected, as the privacy policies may be out of date, or omit collected information.
implementation of a privacy policy in clear and comprehensible non-legalese can help users understand what data is processed by an app and for what purposes. The Working Party is in favor of implementing privacy policies that use language and layouts that are easy to understand.282 There are initiatives specifically tailored for mobile apps, that provide publishers with comprehensible privacy policies which are tailorable to their needs, and that they can easily integrate in their apps.283 The Federal Trade Commission of the United States has also initiated a project to present mobile privacy disclosures in a short, effective and accessible way.284

4.2 e-Privacy Directive

4.2.1 Prior Informed Consent

Article 5 (3) of the e-Privacy Directive states that storage or access to information on terminal equipment of users is only allowed “on [the] condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing”. An exception is made for “any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service”. In §3.3 it was concluded that apps fall within the substantive scope of article 5 (3). In this paragraph, the obligations and exceptions of article 5 (3) will be discussed, followed by a closer look at the interaction of article 5 (3) with the Data Protection Directive.

Two obligations and two exceptions can be found in the provision: (1) obtaining consent from users and (2) providing users with clear and comprehensive information about the purposes of the processing. Article 2 and recital 17 of the e-Privacy Directive state that consent in the e-Privacy Directive, has the same meaning as consent in the Data Protection Directive.285 The

wording of the provision indicates that consent has to be obtained prior to the access or storage of information.\textsuperscript{286} This can be inferred from the phrase “has given [consent]”. The fact that information has to be provided in accordance with the Data Protection Directive, implies that the publisher of an app must conform to the transparency principle of article 10 of the Directive.\textsuperscript{287} The phrase “having been provided with clear and comprehensive information” furthermore indicates that information has to be given to users prior to obtaining consent.\textsuperscript{288} A merge of the these obligations results in prior informed consent.

Prior informed consent is the only ‘legitimate ground’ on which the processing of data that is (to be) stored or accessed on terminal equipment of users can be based. The Working Party notes that when the information - that is processed by means that fall within the scope of article 5 (3) - is also personal data, the Data Protection Directive additionally applies.\textsuperscript{289} This is the result of the Data Protection Directive being a lex generalis in regard to the e-Privacy Directive, as discussed in §3.3. In this regard the Working Party for example acknowledges that the legitimate grounds of the Data Protection Directive are not applicable to article 5 (3), as the provision already specifically covers a legitimate ground: prior informed consent.\textsuperscript{290} As most data that is processed by apps can be deemed personal data, and are accessed on the terminal equipment of users, prior informed consent is the main legitimate ground for apps to process personal data. Zuiderveen Borgesius notes that this could have peculiar consequences when article 5 (3) is applied to cookies.\textsuperscript{291} When prior informed consent is obtained for the storage of and access to cookies on terminal equipment, no additional legitimate grounds of the Data Protection Directive are needed to process personal data that are related to the cookie.\textsuperscript{292} When this interpretation is applied to apps, it would mean that when prior informed consent is obtained to - for example - access the UDID of a user, the subsequent processing of data based on the UDID will not need to be based on additional legitimate grounds of the Data Protection Directive. A different interpretation is discussed by Zuiderveen Borgesius where article 5 (3) would only be a lex

\begin{footnotesize}
\begin{itemize}
  \item[288] WP Opinion 15/2011, p. 31.
  \item[290] WP Opinion 2/2010, p. 10; Debuserre 2005, p. 95.
  \item[291] Zuiderveen Borgesius 2011, p. 7.
  \item[292] Idem.
\end{itemize}
\end{footnotesize}
special is regarding the accessed or stored information. The prior informed consent of article 5 (3) would be adequate to access, for example, the UDID, but any subsequent processing of personal data, save for the UDID itself, would then need to be based on one of the legitimate grounds of the Data Protection Directive.

The fact that the legitimate grounds of the Data Protection Directive do not apply to article 5 (3), furthermore fortifies the argument that consent has to be obtained prior to the data processing. If consent is not obtained prior to the processing of data, there will be a lack of legitimate ground, and the processing would thus be unlawful. If consent is not obtained prior to the data processing, there will be a lack of legitimate ground, and the processing would thus be unlawful.293 Other obligations found in the Data Protection Directive that are not covered in the e-Privacy Directive, such as the principles relating to data quality, do apply.

While (unambiguous) consent has been discussed in the paragraph on legitimate grounds, some additions with regard to prior informed consent need to be made, more specifically on how consent can be obtained. In the discussion of cookies, there have been arguments, especially supported by recital 66 of the Citizens’ Rights Directive, that consent could be obtained by browser settings or through opt-out mechanisms.294 The Working Party has mostly rejected these views.295 Although these two options were (until now) mostly specifically related to cookies, they can be analogized to apps.

The Working Party has stated that prior informed consent cannot be obtained through mandatory acceptance of general terms and conditions, or through opt-out possibilities.296 If opt-out mechanisms would be deemed sufficient to obtain consent, for arguments sake, it is hard to imagine how opt-out mechanisms would be implemented in a mobile environment. Apps differ from websites that store and access cookies for several reasons: first, apps do not merely store or access cookies, but have possibilities to access quite a larger and different set of data. The fact that not all apps access or store the same kind of information (e.g., location data, address book, photos) would result in the need for immensely granular opt-out choices for users. Second, while opting-out with regard to cookies is performed by storing ‘opt-out cookies’, there is no such

293 WP Opinion 15/2011, p. 31.
294 See van Eijk et. al. 2011, p. 3; Recital 66 of the Citizens’ Rights Directive states: “Where it is technically possible and effective, in accordance with the relevant provisions of Directive 95/46/EC, the user’s consent to processing may be expressed by using the appropriate settings of a browser or other application”.
common practice in the mobile environment of apps. While there are no technical difficulties to implement such a system, the uniform implementation of such a system could be troublesome. Regarding browser settings the same difficulties play a role. If browser settings would be deemed sufficient to obtain consent, it is hard to see how that would work in a mobile environment. While all major browsers generally have options regarding the storage of cookies, similar options regarding what data apps can access generally do not exist on mobile operating systems. As described in §4.1.3.1, on Apple’s iOS mobile operating system, no general settings can be found to control what data an app can access, save for location data. As such it is hard to see how ‘mobile operating system settings’ could play a role in obtaining implied consent, even if such settings were deemed appropriate to obtain consent. For a description of how consent can be obtained and what information apps have to provide see §4.1.1.1 and §4.1.4.

Article 5 (3) furthermore stipulates two exceptions that - if applicable - do not require apps to obtain prior informed consent: any technical storage or access for (1) the sole purpose of carrying out the transmission of a communication over an electronic communications network, or (2) as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service. These exceptions are in place to prevent the application of article 5 (3) to any technical storage or access that is required for the above mentioned purposes. There can be discussion about when the exceptions exactly apply, as is demonstrated by the debate on what cookies fall within the exceptions of article 5 (3).297 The first exception can only be invoked in limited circumstances because of its purpose: apps will not easily be able to justify access to data with this exception, especially not where it concerns personal data. The second exception however can lead to discussion about what is strictly necessary for the provided services of an app. If an app provides its users a service that requires the processing of the address book of users, is the processing of the address book strictly necessary for the services provided by the app? Publishers should be cautious in applying the second exception. Even if information such as the address book of users, is strictly necessary for the services provided by an app, by applying the exception - and thus not obtaining the prior informed consent of users - there is no legitimate ground for the processing of the personal data.

They will therefore have to base their processing on the legitimate grounds of the Data Protection Directive, when the accessed or stored information is personal data.

The applicability of article 5 (3) to apps has its implications. Apps generally access data that is already stored on the smart mobile devices of users. As article 5 (3) is a lex specialis of the Data Protection Directive, the main ‘legitimate ground’ to process the above mentioned data is prior informed consent. Therefore, apps can not base their processing on the legitimate grounds of the Data Protection Directive, as long as they process data that fall within the scope of article 5 (3).
5. Conclusion

The first chapter served as an introduction to the world of smart mobile devices, application catalogs and involved stakeholders. The stakeholders consist of vendors of smart mobile devices and application catalogs, third-party app publishers, analytics and advertising companies, and users. First, the chapter gave a description of smart mobile devices and the operation of application catalogs. Second, it showed how third-party apps are developed, the payment models that are available in application catalogs, and what the roles of advertising and analytics companies are. It was established that there is a clear relationship between apps that are based on the free and freemium payment models, and advertising companies. Finally, it also became clear that the legal relationship between users and third-party app publishers are direct. Although the application catalog operators merely sell licenses to use apps, and thus are not directly involved in the legal relationship between users and publishers, they do deem it necessary for publishers of apps that process personal data to notify - and in some cases obtain consent from - users of the processing of their data.

The second chapter consisted of a technical overview of smart mobile devices on several levels. This included what data is available on smart mobile devices, to what extent they are accessible by apps, and what restrictions or requirements there are set in place by operators of application catalogs and mobile operating systems. It revealed that apps on Apple’s iOS mobile operating system can gain access to a wide array of data, often without having to notify users. Depending on the mobile operating system at hand, there are permission models implemented to improve user control in the form of pop-ups or permission lists. In the case of Apple’s iOS, users are only required to give explicit permission for location services via a pop-up, and in the near future also for access to the address book.

The chapter included a technical research to reveal what data is actively or passively processed by apps. The research included seven apps, and was conducted by monitoring the network traffic of apps with the help of the Burp Suite and Wireshark network protocol analyzers. A pseudonym was used to interact with apps by setting up, *inter alia*, an e-mail account and Facebook profile. The results of the research revealed in a concrete way what data is
processed by apps: they ranged from UDIDs to address books and from location data to social media IDs.

The third chapter was dedicated to the applicability and jurisdiction of the Data Protection Directive and the e-Privacy Directive. An evaluation of the data that was processed by the apps that were researched in chapter two, revealed that a majority of the processed data constituted personal data, and that all researched apps processed personal data. It was concluded that when apps process personal data, they fall within the substantive scope of the Data Protection Directive. Regarding jurisdiction, it was concluded that the Data Protection Directive will generally have jurisdiction over publishers of apps that are established within the European Union. The more interesting question was whether the Data Protection Directive can exert jurisdiction over publishers that have no relevant establishment within the European Union. As publishers that have no relevant establishment within the European Union utilize their apps on smart mobile devices, and thus equipment location on Community territory to process personal data, the Data Protection Directive can exert its jurisdiction. Denying the jurisdiction of the Data Protection Directive would create a severe lacunae in the protection of the personal data of millions of European smart mobile device users.

Regarding article 5 (3) of the e-Privacy Directive, it was concluded that apps fall within its substantive scope for two reasons. Firstly, apps can operate exactly as what the rationales behind the provision tries to protect users from: apps can gain access to information without the knowledge of users, store hidden information and track the behavior of users. Secondly, apps access and store information - in most cases personal data - on smart mobile devices of users. As apps also store and access cookies, and thus to the current fame of the provision fall within its substantive scope, it would be a great anomaly to deny the applicability of the provision where it regards other information on smart mobile devices.

The fourth chapter was dedicated to the analysis of the obligations and rights of publishers under the Data Protection Directive and the e-Privacy Directive. First the relevant legitimate grounds on which apps could base their processing of personal data were discussed successively. These legitimate grounds consisted of: unambiguous consent, the necessity for the performance of a contract and the legitimate interest pursued by the app. Regarding the
legitimate ground of unambiguous consent, it was concluded that the current practice of apps to obtain unambiguous consent from users by pop-ups (iOS) or permission lists (Android) can not be deemed sufficient. In order to obtain unambiguous consent, those pop-ups, permission lists and the privacy policies of the apps must provide users with information about how and why their data is processed: a generic permission alone that allows apps to access data can not constitute unambiguous consent from users to the processing of that data.

While apps could possibly base the processing of personal data on the necessity for the performance of a contract, most apps are licensed by a standard license of use which can not form the basis for the processing of personal data as they are generic, and do not contain any information about the services provided by an app or the personal data that is required to be processed by the app. When apps do provide their own EULA, it could possibly form the basis for the processing of personal data, depending on the specific circumstances of the case. The previous statement assumes however that the EULA is a valid contact between the publisher of an app and a user, which remains questionable.

Regarding the ground of legitimate interests, it was concluded that the interests of data subjects weigh heavily, and that therefore controllers will not easily be able to justify their processing on this ground. This is denoted by the fact that information that is stored on smart mobile devices of users are considered to be part of their private sphere, that requires protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms. Users furthermore do not have a lot of control over their data, which in the case of smart mobile devices often consist of a lot of personal data due to the highly personal nature of the devices. It is therefore difficult to imagine that the interests of data subjects do not override the pursued interests of controllers. As smart mobile devices hold a whole range of personal data, it will depend on the circumstances of the case whether an app could justify its processing on the ground of legitimate interest.

The legitimacy and purpose limitation principle of the Data Protection Directive requires apps to clearly stipulate the purposes for which they collect data, and to not further process data in ways that are incompatible with the original purpose that the data was collected for. The proportionality principle furthermore obliges apps to collect data that is adequate, relevant, and
not excessive in relation to the purposes for which they are collected. An evaluation of the researched apps demonstrated that publishers do not always adhere to these principles. Publishers of apps therefore need to question themselves whether they actually need all the data they process, as excessive processing of data is easily achieved on smart mobile devices as the researched apps of chapter two show.

Although apps have an obligation to inform users about what data is processed and for what purposes, the processing is often not transparent to users for three reasons: a lack of a privacy policy, an incorrect or incomplete privacy policy, and the lack of a designated area for users to retrieve privacy policies. This was again demonstrated by the results of the researched apps. An agreement in the United States between the attorney general of California and six leading operators of application catalogs to improve user privacy on smart mobile devices, might improve the transparency issues that are faced. The agreement requires apps to implement privacy policies in case they process personal data, and the operators of application catalogs will provide a designated area within their catalogs for privacy policies. Although most operators of application catalogs already require privacy policies, it can be expected that they will start to enforce these requirements. The effectiveness of the agreement is however yet to be seen. The recent initiatives and guidelines by several parties on mobile privacy could prove to be a helpful and accessible source of information for publishers and developers, although they are not necessarily reconcilable with the obligations of publishers under the Data Protection Directive and the e-Privacy Directive.

As apps fall within the substantive scope of article 5 (3) of the e-Privacy Directive, they are required to obtain prior informed consent from users when they access or store data on smart mobile devices. When the accessed or stored data is also personal data, the Data Protection Directive additionally applies, but only insofar as article 5 (3) does not already specifically cover the matters. A consequence of this is that the main ‘legitimate ground’ for accessing or storing (personal) data on smart mobile devices is prior informed consent. The prior informed consent should however only apply to the processing of the accessed or stored information, and not to any additional processing of personal data based on that information: additional processing should require a legitimate ground based on article 7 of the Data Protection Directive. Where
publishers would like to omit obtaining prior informed consent because the accessed or stored information is necessary for the services provided by the app, they will need to base their processing on the legitimate grounds of the Data Protection Directive, as if there is no prior informed consent or any other legitimate ground, the processing will be illegitimate.

This thesis gave an insight into the problems that surround apps and data protection. The answer to the central research question of this thesis is that publishers of apps need to comply with the Data Protection Directive if they process personal data, and article 5 (3) of the e-Privacy Directive whenever they access or store information on smart mobile devices. Although the technical research in this thesis consisted of a handful of apps, it adequately demonstrated that publishers of apps do not always fulfill their obligations under the Data Protection Directive and the e-Privacy Directive. The research showed that apps are not always transparent about their processing, do not always adhere to the purpose limitation principle and have a tendency to collect data excessively. As prior informed consent is the main applicable ground for a wide range of data that is collected by apps on smart mobile devices, it can also be concluded that apps do not always obtain prior informed consent from users.

There are however several underlying problems of mobile data privacy. First of all, there is a great variety of stakeholders that all have their own interests. Data protection is not always reconcilable with those interests, and seems to fall victim to them. Second, there are a lot of publishers, and an even greater amount of apps. As it is relatively easy for anyone to publish apps, there is a great variety of publishers: apps can be made by a mobile development company with an in-house counsel, or by a teenager. The latter may not have a clue about data protection laws. The former may know all the perks of data protection, but will still not be in full compliance due to the low probability of regulation by data protection authorities. The only question that seems to be relevant is whether an app will be rejected or pulled from an application catalog. Regulating apps, just because of their high volume already, is as hard as regulating websites and poses difficulties. A difference with websites is that application catalogs have gatekeepers: the operators of application catalogs. Whether operators of application catalogs should be forced to play a more active role as gatekeeper is an interesting question. However, operators of application catalogs already took this role on them, by requiring apps that
process personal data to inform their users and obtain their consent. The enforcement of their rules is however lacking. It is therefore interesting to see what the efforts of the attorney general of California will result in, as without the help of application catalogs that can exercise direct and effective power over publishers, regulating apps will be challenging for data protection authorities.

Tackling the problem of mobile data privacy will require involved stakeholders to work together, as applicable data protection laws alone will not overcome the problems at hand. The mobile data privacy conundrum will continue to receive greater attention across the globe - which given the popularity of smart mobile devices and apps is welcome - and hopes that this research can contribute to the debate. Perhaps one day there will be an app for mobile privacy.
Literature list

Directives

**Data Protection Directive**
Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

**Directive 98/34/EC**

**Directive 1999/5/EC**

**e-Privacy Directive**

**Citizens’ Rights Directive**

**Article 29 Working Party**

**WP Privacy on the Internet**

**WP International application**

**WP Opinion 4/2007**

**WP Opinion 1/2008**
WP Opinion 2/2010

WP Opinion 8/2010

WP Opinion 13/2011

WP Opinion 16/2011

WP Opinion 02/2012

Literature

Bø & Pederson 2011

Cleff 2007

Cuijpers & Koops 2008

Debussere 2005

van Eijk et. al. 2011

Good et. al. 2006

Hooghiemstra & Nouwt 2007

Kuner 2007
Leontiadis et. al. 2012

Levis 2011,

Nouwt 2008

Schnabel 2009

Seriot 2010

Sloot & Borgesius 2012

Smith 2010
E. Smith, ‘iPhone Applications & Privacy Issues: An Analysis of Application Transmission of iPhone Unique Device Identifiers (UDIDs)’, 1 October 2010.

Wetherall et. al. 2011

Zevenbergen 2004

Zuiderveen Borgesius 2011

Reports

FTC 2012-1

FTC 2012-2
Appendix A

**Application:** TVGiDS.tv Lite

**Publisher:** MobilePioneers


**EULA:** LAEULA

**Privacy policy:** Available in-app: "The use of this application is completely anonymous".

<table>
<thead>
<tr>
<th>Data</th>
<th>Payload</th>
<th>Permission</th>
<th>Remote host</th>
<th>Hostname</th>
<th>SSL</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDID</td>
<td>159701f3e17e51636a05*</td>
<td>No</td>
<td>216.74.41.14</td>
<td><a href="http://data.flurry.com">data.flurry.com</a></td>
<td>No</td>
</tr>
<tr>
<td>UDID</td>
<td>159701f3e17e51636a05*</td>
<td>No</td>
<td>178.239.60.195</td>
<td><a href="http://ads.tvgids.tv">ads.tvgids.tv</a></td>
<td>No</td>
</tr>
<tr>
<td>UDID</td>
<td>159701f3e17e51636a05*</td>
<td>No</td>
<td>77.245.93.168</td>
<td><a href="http://merlin.nakko.com">merlin.nakko.com</a></td>
<td>No</td>
</tr>
<tr>
<td>UDID</td>
<td>159701f3e17e51636a05*</td>
<td>No</td>
<td>94.245.121.178</td>
<td><a href="http://clk.atdmt.com">clk.atdmt.com</a></td>
<td>No</td>
</tr>
<tr>
<td>Language code</td>
<td>nl_NL</td>
<td>No</td>
<td>216.74.41.14</td>
<td><a href="http://data.flurry.com">data.flurry.com</a></td>
<td>No</td>
</tr>
<tr>
<td>Language code</td>
<td>nl_NL</td>
<td>No</td>
<td>178.239.60.195</td>
<td><a href="http://ads.tvgids.tv">ads.tvgids.tv</a></td>
<td>No</td>
</tr>
<tr>
<td>Language code</td>
<td>nl_NL</td>
<td>No</td>
<td>77.245.93.168</td>
<td><a href="http://merlin.nakko.com">merlin.nakko.com</a></td>
<td>No</td>
</tr>
<tr>
<td>Language code</td>
<td>nl_NL</td>
<td>No</td>
<td>94.245.121.178</td>
<td><a href="http://clk.atdmt.com">clk.atdmt.com</a></td>
<td>No</td>
</tr>
<tr>
<td>Language code</td>
<td>nl_NL</td>
<td>No</td>
<td>77.245.93.168</td>
<td><a href="http://folders.nakko.com">folders.nakko.com</a></td>
<td>No</td>
</tr>
<tr>
<td>OS version</td>
<td>5.0</td>
<td>No</td>
<td>178.239.60.195</td>
<td><a href="http://ads.tvgids.tv">ads.tvgids.tv</a></td>
<td>No</td>
</tr>
<tr>
<td>OS version</td>
<td>5.0</td>
<td>No</td>
<td>77.245.93.168</td>
<td><a href="http://merlin.nakko.com">merlin.nakko.com</a></td>
<td>No</td>
</tr>
<tr>
<td>OS version</td>
<td>5.0</td>
<td>No</td>
<td>94.245.121.178</td>
<td><a href="http://clk.atdmt.com">clk.atdmt.com</a></td>
<td>No</td>
</tr>
<tr>
<td>OS version</td>
<td>5.0</td>
<td>No</td>
<td>77.245.93.168</td>
<td><a href="http://folders.nakko.com">folders.nakko.com</a></td>
<td>No</td>
</tr>
<tr>
<td>Device name</td>
<td>Sinon Aesimus’ iPhone</td>
<td>No</td>
<td>178.239.60.195</td>
<td><a href="http://ads.tvgids.tv">ads.tvgids.tv</a></td>
<td>No</td>
</tr>
<tr>
<td>Device name</td>
<td>Sinon Aesimus’ iPhone</td>
<td>No</td>
<td>77.245.93.168</td>
<td><a href="http://merlin.nakko.com">merlin.nakko.com</a></td>
<td>No</td>
</tr>
<tr>
<td>Device name</td>
<td>Sinon Aesimus’ iPhone</td>
<td>No</td>
<td>94.245.121.178</td>
<td><a href="http://clk.atdmt.com">clk.atdmt.com</a></td>
<td>No</td>
</tr>
<tr>
<td>Device name</td>
<td>Sinon Aesimus’ iPhone</td>
<td>No</td>
<td>77.245.93.168</td>
<td><a href="http://folders.nakko.com">folders.nakko.com</a></td>
<td>No</td>
</tr>
<tr>
<td>Device model</td>
<td>iPhone4,1</td>
<td>No</td>
<td>216.74.41.14</td>
<td><a href="http://data.flurry.com">data.flurry.com</a></td>
<td>No</td>
</tr>
<tr>
<td>Device model</td>
<td>iPhone4,1</td>
<td>No</td>
<td>178.239.60.195</td>
<td><a href="http://ads.tvgids.tv">ads.tvgids.tv</a></td>
<td>No</td>
</tr>
<tr>
<td>Device model</td>
<td>iPhone4,1</td>
<td>No</td>
<td>77.245.93.168</td>
<td><a href="http://merlin.nakko.com">merlin.nakko.com</a></td>
<td>No</td>
</tr>
<tr>
<td>Device model</td>
<td>iPhone4,1</td>
<td>No</td>
<td>94.245.121.178</td>
<td><a href="http://clk.atdmt.com">clk.atdmt.com</a></td>
<td>No</td>
</tr>
<tr>
<td>Device model</td>
<td>iPhone4,1</td>
<td>No</td>
<td>77.245.93.168</td>
<td><a href="http://folders.nakko.com">folders.nakko.com</a></td>
<td>No</td>
</tr>
<tr>
<td>Device model</td>
<td>iPhone4,1</td>
<td>No</td>
<td>74.125.232.250</td>
<td><a href="http://googleads.g.doubleclick.net">googleads.g.doubleclick.net</a></td>
<td>No</td>
</tr>
<tr>
<td>Device model</td>
<td>iPhone4,1</td>
<td>No</td>
<td>74.125.232.223</td>
<td><a href="http://media.admob.com">media.admob.com</a></td>
<td>No</td>
</tr>
<tr>
<td>WiFi/3G</td>
<td>WiFi</td>
<td>No</td>
<td>178.239.60.195</td>
<td><a href="http://ads.tvgids.tv">ads.tvgids.tv</a></td>
<td>No</td>
</tr>
<tr>
<td>WiFi/3G</td>
<td>WiFi</td>
<td>No</td>
<td>77.245.93.168</td>
<td><a href="http://merlin.nakko.com">merlin.nakko.com</a></td>
<td>No</td>
</tr>
<tr>
<td>WiFi/3G</td>
<td>WiFi</td>
<td>No</td>
<td>94.245.121.178</td>
<td><a href="http://clk.atdmt.com">clk.atdmt.com</a></td>
<td>No</td>
</tr>
<tr>
<td>WiFi/3G</td>
<td>WiFi</td>
<td>No</td>
<td>77.245.93.168</td>
<td><a href="http://folders.nakko.com">folders.nakko.com</a></td>
<td>No</td>
</tr>
<tr>
<td>Timezone</td>
<td>Europe/Prague</td>
<td>No</td>
<td>216.74.41.14</td>
<td><a href="http://data.flurry.com">data.flurry.com</a></td>
<td>No</td>
</tr>
</tbody>
</table>

![Figure A.1 TVGiDS.tv Lite](image)

298 **Table explanation**

*Data:* The type of data that was processed.

*Payload:* The actual data that is sent to a receiving host.

*Permission:* This concerns explicit permission. Yes represents that permission was asked and granted. No represent that no permission was asked and thus no permission was and could be granted. User represents user-entered obliged data. Optional represents user-entered optional data.

*Remote host:* The IP-address of the receiving host.

*Hostname:* The local hostname and domain name of the host in a HTTP(S)-header.

*SSL:* Whether the connection was secured with SSL.
### Application
TVGiDS.tv

### Publisher
MobilePioneers

### iTunes link

### EULA
LAEULA

### Privacy policy

<table>
<thead>
<tr>
<th>Data</th>
<th>Payload</th>
<th>Permission</th>
<th>Remote host</th>
<th>Hostname</th>
<th>SSL</th>
<th>Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDID</td>
<td>159701f3e1e51636a05*</td>
<td>No</td>
<td>216.74.41.14</td>
<td><a href="http://data.flurry.com">http://data.flurry.com</a></td>
<td>No</td>
<td>Flurry</td>
</tr>
<tr>
<td>UDID</td>
<td>159701f3e1e51636a05*</td>
<td>No</td>
<td>178.22.59.7</td>
<td><a href="http://www.tvgids.tv">http://www.tvgids.tv</a></td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>UDID</td>
<td>9f46366063da837e5c*</td>
<td>No</td>
<td>178.22.59.7</td>
<td><a href="http://www.tvgids.tv">http://www.tvgids.tv</a></td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>UDID</td>
<td>159701f3e1e51636a05*</td>
<td>No</td>
<td>78.136.3.145</td>
<td><a href="http://betclic.12snap.mobi">http://betclic.12snap.mobi</a></td>
<td>No</td>
<td>12snap</td>
</tr>
<tr>
<td>UDID</td>
<td>9f46366063da837e5c*</td>
<td>No</td>
<td>78.136.3.145</td>
<td><a href="http://betclic.12snap.mobi">http://betclic.12snap.mobi</a></td>
<td>No</td>
<td>12snap</td>
</tr>
<tr>
<td>UDID</td>
<td>159701f3e1e51636a05*</td>
<td>No</td>
<td>77.245.93.168</td>
<td><a href="http://merlin.nakko.com">http://merlin.nakko.com</a></td>
<td>No</td>
<td>Nakko</td>
</tr>
<tr>
<td>UDID</td>
<td>9f46366063da837e5c*</td>
<td>No</td>
<td>77.245.93.168</td>
<td><a href="http://merlin.nakko.com">http://merlin.nakko.com</a></td>
<td>No</td>
<td>Nakko</td>
</tr>
<tr>
<td>UDID</td>
<td>159701f3e1e51636a05*</td>
<td>No</td>
<td>77.245.93.168</td>
<td><a href="http://foldersnl.nakko.com">http://foldersnl.nakko.com</a></td>
<td>No</td>
<td>Nakko</td>
</tr>
<tr>
<td>UDID</td>
<td>9f46366063da837e5c*</td>
<td>No</td>
<td>77.245.93.168</td>
<td><a href="http://foldersnl.nakko.com">http://foldersnl.nakko.com</a></td>
<td>No</td>
<td>Nakko</td>
</tr>
<tr>
<td>UDID</td>
<td>159701f3e1e51636a05*</td>
<td>No</td>
<td>178.239.60.17</td>
<td><a href="http://ads.iphone-marketing.nl">http://ads.iphone-marketing.nl</a></td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>UDID</td>
<td>9f46366063da837e5c*</td>
<td>No</td>
<td>178.239.60.17</td>
<td><a href="http://ads.iphone-marketing.nl">http://ads.iphone-marketing.nl</a></td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Device name</td>
<td>Sinon Aesimus’ iPhone</td>
<td>No</td>
<td>78.136.3.145</td>
<td><a href="http://betclic.12snap.mobi">http://betclic.12snap.mobi</a></td>
<td>No</td>
<td>12snap</td>
</tr>
<tr>
<td>Device name</td>
<td>Sinon Aesimus’ iPhone</td>
<td>No</td>
<td>77.245.93.168</td>
<td><a href="http://merlin.nakko.com">http://merlin.nakko.com</a></td>
<td>No</td>
<td>Nakko</td>
</tr>
<tr>
<td>Device name</td>
<td>Sinon Aesimus’ iPhone</td>
<td>No</td>
<td>77.245.93.168</td>
<td><a href="http://foldersnl.nakko.com">http://foldersnl.nakko.com</a></td>
<td>No</td>
<td>Nakko</td>
</tr>
<tr>
<td>Device name</td>
<td>Sinon Aesimus’ iPhone</td>
<td>No</td>
<td>178.239.60.17</td>
<td><a href="http://ads.iphone-marketing.nl">http://ads.iphone-marketing.nl</a></td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Device name</td>
<td>Sinon Aesimus’ iPhone</td>
<td>No</td>
<td>178.22.59.7</td>
<td><a href="http://www.tvgids.tv">http://www.tvgids.tv</a></td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Device model</td>
<td>iPhone4,1</td>
<td>No</td>
<td>216.74.41.14</td>
<td><a href="http://data.flurry.com">http://data.flurry.com</a></td>
<td>No</td>
<td>Flurry</td>
</tr>
<tr>
<td>Device model</td>
<td>iPhone4,1</td>
<td>No</td>
<td>78.136.3.145</td>
<td><a href="http://betclic.12snap.mobi">http://betclic.12snap.mobi</a></td>
<td>No</td>
<td>12snap</td>
</tr>
<tr>
<td>Device model</td>
<td>iPhone4,1</td>
<td>No</td>
<td>77.245.93.168</td>
<td><a href="http://merlin.nakko.com">http://merlin.nakko.com</a></td>
<td>No</td>
<td>Nakko</td>
</tr>
<tr>
<td>Device model</td>
<td>iPhone4,1</td>
<td>No</td>
<td>77.245.93.168</td>
<td><a href="http://foldersnl.nakko.com">http://foldersnl.nakko.com</a></td>
<td>No</td>
<td>Nakko</td>
</tr>
<tr>
<td>Device model</td>
<td>iPhone4,1</td>
<td>No</td>
<td>178.239.60.17</td>
<td><a href="http://ads.iphone-marketing.nl">http://ads.iphone-marketing.nl</a></td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Device model</td>
<td>iPhone4,1</td>
<td>No</td>
<td>178.22.59.7</td>
<td><a href="http://www.tvgids.tv">http://www.tvgids.tv</a></td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>OS version</td>
<td>5.0</td>
<td>No</td>
<td>77.245.93.168</td>
<td><a href="http://merlin.nakko.com">http://merlin.nakko.com</a></td>
<td>No</td>
<td>Nakko</td>
</tr>
<tr>
<td>OS version</td>
<td>5.0</td>
<td>No</td>
<td>78.136.3.145</td>
<td><a href="http://betclic.12snap.mobi">http://betclic.12snap.mobi</a></td>
<td>No</td>
<td>12snap</td>
</tr>
<tr>
<td>OS version</td>
<td>5.0</td>
<td>No</td>
<td>77.245.93.168</td>
<td><a href="http://foldersnl.nakko.com">http://foldersnl.nakko.com</a></td>
<td>No</td>
<td>Nakko</td>
</tr>
<tr>
<td>OS version</td>
<td>5.0</td>
<td>No</td>
<td>178.239.60.17</td>
<td><a href="http://ads.iphone-marketing.nl">http://ads.iphone-marketing.nl</a></td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Language code</td>
<td>nl_NL</td>
<td>No</td>
<td>216.74.41.14</td>
<td><a href="http://data.flurry.com">http://data.flurry.com</a></td>
<td>No</td>
<td>Flurry</td>
</tr>
<tr>
<td>Language code</td>
<td>nl_NL</td>
<td>No</td>
<td>77.245.93.168</td>
<td><a href="http://merlin.nakko.com">http://merlin.nakko.com</a></td>
<td>No</td>
<td>Nakko</td>
</tr>
<tr>
<td>Language code</td>
<td>nl_NL</td>
<td>No</td>
<td>77.245.93.168</td>
<td><a href="http://foldersnl.nakko.com">http://foldersnl.nakko.com</a></td>
<td>No</td>
<td>Nakko</td>
</tr>
<tr>
<td>Language code</td>
<td>nl_NL</td>
<td>No</td>
<td>178.239.60.17</td>
<td><a href="http://ads.iphone-marketing.nl">http://ads.iphone-marketing.nl</a></td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Language code</td>
<td>nl_NL</td>
<td>No</td>
<td>178.22.59.7</td>
<td><a href="http://www.tvgids.tv">http://www.tvgids.tv</a></td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Language code</td>
<td>nl_NL</td>
<td>No</td>
<td>78.136.3.145</td>
<td><a href="http://betclic.12snap.mobi">http://betclic.12snap.mobi</a></td>
<td>No</td>
<td>12snap</td>
</tr>
<tr>
<td>WiFi/3G</td>
<td>WiFi</td>
<td>No</td>
<td>78.136.3.145</td>
<td><a href="http://betclic.12snap.mobi">http://betclic.12snap.mobi</a></td>
<td>No</td>
<td>12snap</td>
</tr>
<tr>
<td>WiFi/3G</td>
<td>WiFi</td>
<td>No</td>
<td>77.245.93.168</td>
<td><a href="http://merlin.nakko.com">http://merlin.nakko.com</a></td>
<td>No</td>
<td>Nakko</td>
</tr>
<tr>
<td>WiFi/3G</td>
<td>WiFi</td>
<td>No</td>
<td>77.245.93.168</td>
<td><a href="http://foldersnl.nakko.com">http://foldersnl.nakko.com</a></td>
<td>No</td>
<td>Nakko</td>
</tr>
<tr>
<td>WiFi/3G</td>
<td>WiFi</td>
<td>No</td>
<td>178.239.60.17</td>
<td><a href="http://ads.iphone-marketing.nl">http://ads.iphone-marketing.nl</a></td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>WiFi/3G</td>
<td>WiFi</td>
<td>No</td>
<td>178.22.59.7</td>
<td><a href="http://www.tvgids.tv">http://www.tvgids.tv</a></td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Timezone</td>
<td>Europe/Prague</td>
<td>No</td>
<td>216.74.41.14</td>
<td><a href="http://data.flurry.com">http://data.flurry.com</a></td>
<td>No</td>
<td>Flurry</td>
</tr>
</tbody>
</table>

Figure A.2 TVGiDS.tv
**Application:** NU

**Publisher:** Peperzaken


**EULA:** LAEULA


<table>
<thead>
<tr>
<th>Data</th>
<th>Payload</th>
<th>Permission</th>
<th>Remote host</th>
<th>Hostname</th>
<th>SSL</th>
<th>Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDID</td>
<td>159701f3e17e51636a05*</td>
<td>No</td>
<td>216.74.41.14</td>
<td><a href="http://data.flurry.com">http://data.flurry.com</a></td>
<td>No</td>
<td>Flurry</td>
</tr>
<tr>
<td>UDID</td>
<td>159701f3e17e51636a05*</td>
<td>No</td>
<td>62.69.175.18</td>
<td><a href="http://app.nu.nl">http://app.nu.nl</a></td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>UDID</td>
<td>159701f3e17e51636a05*</td>
<td>No</td>
<td>77.245.84.9</td>
<td><a href="http://eu1.madsone.com">http://eu1.madsone.com</a></td>
<td>No</td>
<td>MADS</td>
</tr>
<tr>
<td>Location</td>
<td>(50.x, 14.x)</td>
<td>Yes</td>
<td>77.245.84.9</td>
<td><a href="http://eu1.madsone.com">http://eu1.madsone.com</a></td>
<td>No</td>
<td>MADS</td>
</tr>
<tr>
<td>WiFi/3G</td>
<td>WiFi</td>
<td>No</td>
<td>77.245.84.9</td>
<td><a href="http://eu1.madsone.com">http://eu1.madsone.com</a></td>
<td>No</td>
<td>MADS</td>
</tr>
<tr>
<td>Timezone</td>
<td>Europe/Prague</td>
<td>No</td>
<td>216.74.41.14</td>
<td><a href="http://data.flurry.com">http://data.flurry.com</a></td>
<td>No</td>
<td>Flurry</td>
</tr>
</tbody>
</table>

**Figure A.3 NU**

**Application:** Dosecast

**Publisher:** Montuno Software, LLC


**EULA:** Available on iTunes and in-app. Different version available on website: [http://www.dosecast.com/terms.html](http://www.dosecast.com/terms.html). Requires explicit consent from user to EULA in order to use application.

**Privacy policy:** Fully incorporated in to EULA.

<table>
<thead>
<tr>
<th>Data</th>
<th>Payload</th>
<th>Permission</th>
<th>Remote host</th>
<th>Hostname</th>
<th>SSL</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDID</td>
<td>159701f3e17e51636a05*</td>
<td>No</td>
<td>50.17.238.75</td>
<td><a href="https://ppserver.montunosoftware.com">https://ppserver.montunosoftware.com</a></td>
<td>Yes</td>
</tr>
<tr>
<td>OS version</td>
<td>5.0</td>
<td>No</td>
<td>50.17.238.75</td>
<td><a href="https://ppserver.montunosoftware.com">https://ppserver.montunosoftware.com</a></td>
<td>Yes</td>
</tr>
<tr>
<td>Language code</td>
<td>nl_NL</td>
<td>No</td>
<td>50.17.238.75</td>
<td><a href="https://ppserver.montunosoftware.com">https://ppserver.montunosoftware.com</a></td>
<td>Yes</td>
</tr>
<tr>
<td>Device type</td>
<td>iPhone</td>
<td>No</td>
<td>50.17.238.75</td>
<td><a href="https://ppserver.montunosoftware.com">https://ppserver.montunosoftware.com</a></td>
<td>Yes</td>
</tr>
<tr>
<td>Language code</td>
<td>en_NL</td>
<td>No</td>
<td>50.17.238.75</td>
<td><a href="https://ppserver.montunosoftware.com">https://ppserver.montunosoftware.com</a></td>
<td>Yes</td>
</tr>
<tr>
<td>Timezone</td>
<td>Europe/Prague</td>
<td>No</td>
<td>50.17.238.75</td>
<td><a href="https://ppserver.montunosoftware.com">https://ppserver.montunosoftware.com</a></td>
<td>Yes</td>
</tr>
<tr>
<td>Doctor</td>
<td>x</td>
<td>No</td>
<td>50.17.238.75</td>
<td><a href="https://ppserver.montunosoftware.com">https://ppserver.montunosoftware.com</a></td>
<td>Yes</td>
</tr>
<tr>
<td>Pharmacy</td>
<td>x</td>
<td>No</td>
<td>50.17.238.75</td>
<td><a href="https://ppserver.montunosoftware.com">https://ppserver.montunosoftware.com</a></td>
<td>Yes</td>
</tr>
<tr>
<td>Drug</td>
<td>x</td>
<td>No</td>
<td>50.17.238.75</td>
<td><a href="https://ppserver.montunosoftware.com">https://ppserver.montunosoftware.com</a></td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Figure A.4 Dosecast**
Application: Angry Birds Free
Publisher: Rovio Mobile Ltd.
EULA: LAEULA
Privacy policy: Available in-app at [http://www.rovio.com/Privacy](http://www.rovio.com/Privacy)

<table>
<thead>
<tr>
<th>Data</th>
<th>Payload</th>
<th>Permission</th>
<th>Remote host</th>
<th>Hostname</th>
<th>SSL</th>
<th>Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDID</td>
<td>677FDD41EDE69CC243*</td>
<td>No</td>
<td>205.139.101.150</td>
<td><a href="http://admax.nexage.com">http://admax.nexage.com</a></td>
<td>No</td>
<td>Nexage</td>
</tr>
<tr>
<td>UDID</td>
<td>d9f284f1dfb677abe016d*</td>
<td>No</td>
<td>205.139.101.150</td>
<td><a href="http://admax.nexage.com">http://admax.nexage.com</a></td>
<td>No</td>
<td>Nexage</td>
</tr>
<tr>
<td>UDID</td>
<td>159701f3e17e51636a05*</td>
<td>No</td>
<td>216.74.41.14</td>
<td><a href="http://data.flurry.com">http://data.flurry.com</a></td>
<td>No</td>
<td>Flurry</td>
</tr>
<tr>
<td>UDID</td>
<td>d9f284f1dfb677abe016d*</td>
<td>No</td>
<td>2.21.246.103</td>
<td><a href="http://ads.mojiva.com">http://ads.mojiva.com</a></td>
<td>No</td>
<td>Mojiva</td>
</tr>
<tr>
<td>UDID</td>
<td>d9f284f1dfb677abe016d*</td>
<td>No</td>
<td>67.228.26.194</td>
<td><a href="http://ads.mdotm.com">http://ads.mdotm.com</a></td>
<td>No</td>
<td>Mdotm</td>
</tr>
<tr>
<td>UDID</td>
<td>159701f3e17e51636a05*</td>
<td>No</td>
<td>95.100.163.120</td>
<td>[<a href="https://iad">https://iad</a> sdk.apple.com](<a href="https://iad">https://iad</a> sdk.apple.com)</td>
<td>Yes</td>
<td>Apple Ads</td>
</tr>
<tr>
<td>UDID</td>
<td>d9f284f1dfb677abe016d*</td>
<td>No</td>
<td>208.43.117.85</td>
<td><a href="http://rtb.nexage.com">http://rtb.nexage.com</a></td>
<td>No</td>
<td>Nexage</td>
</tr>
<tr>
<td>UDID</td>
<td>d9f284f1dfb677abe016d*</td>
<td>No</td>
<td>95.172.8.135</td>
<td><a href="http://adfonic.net">http://adfonic.net</a></td>
<td>No</td>
<td>Adfonic</td>
</tr>
<tr>
<td>IP-address</td>
<td>62.24.**</td>
<td>No</td>
<td>205.139.101.150</td>
<td><a href="http://admax.nexage.com">http://admax.nexage.com</a></td>
<td>No</td>
<td>Nexage</td>
</tr>
<tr>
<td>IP-address</td>
<td>62.24.**</td>
<td>No</td>
<td>64.236.144.229</td>
<td><a href="http://adserver.adtechus.com">http://adserver.adtechus.com</a></td>
<td>No</td>
<td>Nexage</td>
</tr>
<tr>
<td>IP-address</td>
<td>62.24.**</td>
<td>No</td>
<td>2.21.246.103</td>
<td><a href="http://ads.mojiva.com">http://ads.mojiva.com</a></td>
<td>No</td>
<td>Mojiva</td>
</tr>
<tr>
<td>IP-address</td>
<td>62.24.**</td>
<td>No</td>
<td>209.94.144.164</td>
<td><a href="http://s.jumptap.com">http://s.jumptap.com</a></td>
<td>No</td>
<td>Jumptap</td>
</tr>
<tr>
<td>IP-address</td>
<td>62.24.**</td>
<td>No</td>
<td>83.138.173.60</td>
<td><a href="http://ww.inmobi.com">http://ww.inmobi.com</a></td>
<td>No</td>
<td>Inmobi</td>
</tr>
<tr>
<td>IP-address</td>
<td>62.24.**</td>
<td>No</td>
<td>208.43.117.85</td>
<td><a href="http://rtb.nexage.com">http://rtb.nexage.com</a></td>
<td>No</td>
<td>Nexage</td>
</tr>
<tr>
<td>IP-address</td>
<td>62.24.**</td>
<td>No</td>
<td>95.172.8.135</td>
<td><a href="http://ad2.adfonic.net">http://ad2.adfonic.net</a></td>
<td>No</td>
<td>Adfonic</td>
</tr>
<tr>
<td>IP-address</td>
<td>62.24.**</td>
<td>No</td>
<td>95.172.8.135</td>
<td><a href="http://ad2.adfonic.net">http://ad2.adfonic.net</a></td>
<td>No</td>
<td>Adfonic</td>
</tr>
<tr>
<td>Device model</td>
<td>iPhone4,1</td>
<td>No</td>
<td>74.125.232.250</td>
<td><a href="http://www.chillingo-crystal.appspot.com">http://www.chillingo-crystal.appspot.com</a></td>
<td>Yes</td>
<td>Millennial</td>
</tr>
<tr>
<td>Language code</td>
<td>nl_NL</td>
<td>No</td>
<td>216.74.41.14</td>
<td><a href="http://data.flurry.com">http://data.flurry.com</a></td>
<td>No</td>
<td>Flurry</td>
</tr>
<tr>
<td>Timezone</td>
<td>Europe/Prague</td>
<td>No</td>
<td>216.74.41.14</td>
<td><a href="http://data.flurry.com">http://data.flurry.com</a></td>
<td>No</td>
<td>Flurry</td>
</tr>
</tbody>
</table>

**Figure A.5 Angry Birds Free**

Application: Little Lost Chick Lite
Publisher: Clickgamer Technologies Ltd.
EULA: LAEULA
Privacy policy: Available in-app for use of Chillingo Crystal social gaming platform.

<table>
<thead>
<tr>
<th>Data</th>
<th>Payload</th>
<th>Permission</th>
<th>Remote host</th>
<th>Hostname</th>
<th>SSL</th>
<th>Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDID</td>
<td>159701f3e17e51636a05*</td>
<td>Yes</td>
<td>209.85.173.141</td>
<td><a href="https://chillingo-crystal.appspot.com">https://chillingo-crystal.appspot.com</a></td>
<td>No</td>
<td>Chillingo</td>
</tr>
<tr>
<td>Location</td>
<td>(50.x, 14.x)</td>
<td>Yes</td>
<td>209.85.173.141</td>
<td><a href="https://chillingo-crystal.appspot.com">https://chillingo-crystal.appspot.com</a></td>
<td>Yes</td>
<td>Chillingo</td>
</tr>
<tr>
<td>Address book</td>
<td>First, Last, Phone number</td>
<td>No</td>
<td>209.85.173.141</td>
<td><a href="https://chillingo-crystal.appspot.com">https://chillingo-crystal.appspot.com</a></td>
<td>Yes</td>
<td>Chillingo</td>
</tr>
<tr>
<td>E-mail</td>
<td><a href="mailto:sinon.aesimus@gmail.com">sinon.aesimus@gmail.com</a></td>
<td>User</td>
<td>209.85.173.141</td>
<td><a href="https://chillingo-crystal.appspot.com">https://chillingo-crystal.appspot.com</a></td>
<td>Yes</td>
<td>Chillingo</td>
</tr>
<tr>
<td>Username</td>
<td>sinon.aesimus</td>
<td>User</td>
<td>209.85.173.141</td>
<td><a href="https://chillingo-crystal.appspot.com">https://chillingo-crystal.appspot.com</a></td>
<td>Yes</td>
<td>Chillingo</td>
</tr>
<tr>
<td>Gamecenter ID</td>
<td>Sinon Aesimus</td>
<td>No</td>
<td>209.85.173.141</td>
<td><a href="https://chillingo-crystal.appspot.com">https://chillingo-crystal.appspot.com</a></td>
<td>Yes</td>
<td>Chillingo</td>
</tr>
<tr>
<td>Profile picture</td>
<td>-</td>
<td>Optional</td>
<td>209.85.173.141</td>
<td><a href="https://chillingo-crystal.appspot.com">https://chillingo-crystal.appspot.com</a></td>
<td>Yes</td>
<td>Chillingo</td>
</tr>
<tr>
<td>Facebook ID</td>
<td>10000317601976</td>
<td>Optional</td>
<td>209.85.173.141</td>
<td><a href="https://chillingo-crystal.appspot.com">https://chillingo-crystal.appspot.com</a></td>
<td>Yes</td>
<td>Chillingo</td>
</tr>
<tr>
<td>Device model</td>
<td>iPhone4,1</td>
<td>No</td>
<td>209.85.173.141</td>
<td><a href="https://chillingo-crystal.appspot.com">https://chillingo-crystal.appspot.com</a></td>
<td>Yes</td>
<td>Chillingo</td>
</tr>
</tbody>
</table>

**Figure A.6 Little Lost Chick Lite**
Application: Blood and Glory
Publisher: Glu Games Inc.

iTunes link: http://itunes.apple.com/gb/app/blood-glory/id466067444?mt=8


<table>
<thead>
<tr>
<th>Data</th>
<th>Payload</th>
<th>Permission</th>
<th>Remote host</th>
<th>Hostname</th>
<th>SSL</th>
<th>Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDID</td>
<td>159701f3e17e51636a05*</td>
<td>No</td>
<td>67.214.210.54</td>
<td><a href="https://api.openfeint.com">https://api.openfeint.com</a></td>
<td>Yes</td>
<td>Openfeint</td>
</tr>
<tr>
<td>UDID</td>
<td>159701f3e17e51636a05*</td>
<td>No</td>
<td>216.74.41.14</td>
<td><a href="http://data.flurry.com">http://data.flurry.com</a></td>
<td>No</td>
<td>Flurry</td>
</tr>
<tr>
<td>UDID</td>
<td>159701f3e17e51636a05*</td>
<td>No</td>
<td>184.72.48.104</td>
<td><a href="http://api2.playhaven.com">http://api2.playhaven.com</a></td>
<td>No</td>
<td>Playhaven</td>
</tr>
<tr>
<td>UDID</td>
<td>159701f3e17e51636a05*</td>
<td>No</td>
<td>184.73.170.206</td>
<td><a href="http://ads.admarvel.com">http://ads.admarvel.com</a></td>
<td>No</td>
<td>Admarvel</td>
</tr>
<tr>
<td>UDID</td>
<td>159701f3e17e51636a05*</td>
<td>No</td>
<td>174.129.218.0</td>
<td><a href="https://ws.tapjoyads.com">https://ws.tapjoyads.com</a></td>
<td>Yes</td>
<td>Tapjoy</td>
</tr>
<tr>
<td>MAC-address</td>
<td>68a86d*</td>
<td>No</td>
<td>174.129.218.0</td>
<td><a href="https://ws.tapjoyads.com">https://ws.tapjoyads.com</a></td>
<td>Yes</td>
<td>Tapjoy</td>
</tr>
<tr>
<td>Device name</td>
<td>Sinon Aesimus’ iPhone</td>
<td>No</td>
<td>67.214.210.54</td>
<td><a href="https://api.openfeint.com">https://api.openfeint.com</a></td>
<td>Yes</td>
<td>Openfeint</td>
</tr>
<tr>
<td>Device model</td>
<td>iPhone4,1</td>
<td>No</td>
<td>184.72.48.104</td>
<td><a href="http://api2.playhaven.com">http://api2.playhaven.com</a></td>
<td>No</td>
<td>Playhaven</td>
</tr>
<tr>
<td>Device model</td>
<td>iPhone4,1</td>
<td>No</td>
<td>184.73.170.206</td>
<td><a href="http://ads.admarvel.com">http://ads.admarvel.com</a></td>
<td>No</td>
<td>Admarvel</td>
</tr>
<tr>
<td>Device model</td>
<td>iPhone4,1</td>
<td>No</td>
<td>174.129.218.0</td>
<td><a href="https://ws.tapjoyads.com">https://ws.tapjoyads.com</a></td>
<td>Yes</td>
<td>Tapjoy</td>
</tr>
<tr>
<td>OS version</td>
<td>5.0</td>
<td>No</td>
<td>67.214.210.54</td>
<td><a href="https://api.openfeint.com">https://api.openfeint.com</a></td>
<td>Yes</td>
<td>Openfeint</td>
</tr>
<tr>
<td>OS version</td>
<td>5.0</td>
<td>No</td>
<td>184.72.48.104</td>
<td><a href="http://api2.playhaven.com">http://api2.playhaven.com</a></td>
<td>No</td>
<td>Playhaven</td>
</tr>
<tr>
<td>OS version</td>
<td>5.0</td>
<td>No</td>
<td>184.73.170.206</td>
<td><a href="http://ads.admarvel.com">http://ads.admarvel.com</a></td>
<td>No</td>
<td>Admarvel</td>
</tr>
<tr>
<td>OS version</td>
<td>5.0</td>
<td>No</td>
<td>174.129.218.0</td>
<td><a href="https://ws.tapjoyads.com">https://ws.tapjoyads.com</a></td>
<td>Yes</td>
<td>Tapjoy</td>
</tr>
<tr>
<td>Carrier name</td>
<td>vf nl (Vodafone NL)</td>
<td>No</td>
<td>174.129.218.0</td>
<td><a href="https://ws.tapjoyads.com">https://ws.tapjoyads.com</a></td>
<td>Yes</td>
<td>Tapjoy</td>
</tr>
<tr>
<td>MCC</td>
<td>204</td>
<td>No</td>
<td>174.129.218.0</td>
<td><a href="https://ws.tapjoyads.com">https://ws.tapjoyads.com</a></td>
<td>Yes</td>
<td>Tapjoy</td>
</tr>
<tr>
<td>MNC</td>
<td>4</td>
<td>No</td>
<td>174.129.218.0</td>
<td><a href="https://ws.tapjoyads.com">https://ws.tapjoyads.com</a></td>
<td>Yes</td>
<td>Tapjoy</td>
</tr>
<tr>
<td>CCC</td>
<td>NL</td>
<td>No</td>
<td>174.129.218.0</td>
<td><a href="https://ws.tapjoyads.com">https://ws.tapjoyads.com</a></td>
<td>Yes</td>
<td>Tapjoy</td>
</tr>
<tr>
<td>WiFi/3G</td>
<td>WiFi</td>
<td>No</td>
<td>184.73.170.206</td>
<td><a href="http://ads.admarvel.com">http://ads.admarvel.com</a></td>
<td>No</td>
<td>Admarvel</td>
</tr>
</tbody>
</table>

Figure A.7 Blood and Glory