COLLEGE BESCHERMING PERSOONSGEGEVENS

POSTAL ADDRESS PO Box 93374, 2509 AJ The Hague VISITING ADDRESS Juliana van Stolberglaan 4-10
TEL 070 - 88 88 500 FAX 070 - 88 88 501 INTERNET www.cbpweb.nl www.mijnprivacy.nl

Dutch Data Protection Authority

Investigation into the processing of personal data for the 'whatsapp' mobile application by WhatsApp Inc.

Z2011-00987

Report on the definitive findings

January 2013

PUBLIC VERSION

DATE 15 January 2013

TABLE OF CONTENTS

SUMMARY

Together with the Canadian regulator Office of the Privacy Commissioner of Canada (hereinafter called OPC), the Dutch Data Protection Authority (Dutch DPA) [College bescherming persoonsgegevens] has launched an investigation into the processing of personal data by WhatsApp Inc. (hereinafter called WhatsApp), the developer of the 'whatsapp' mobile communication application (app).

WhatsApp is based in California in the United States. The whatsapp app is a widely-used instant messaging application for smartphones. The app was designed as a free Internet alternative to SMS and is available for a range of smartphones and operating systems, including Apple's iPhone, Microsoft's Windows Phone, Research in Motion's Blackberry, Nokia's Symbian and S40 and devices equipped with Google's Android operating system. Users can also use whatsapp to send and receive photographs, videos and audio files (MMS).

The whatsapp app for the iPhone can be purchased for a one-off fee of EUR 0.89. On other operating systems, the app is free for the first year. The app can be used to send and receive messages free of charge. Users pay only the costs of data use over the Internet.

The app is very popular worldwide and is one of the world's top five best-selling apps. According to WhatsApp, since October 2011 more than a billion messages have been sent through the app every day.

Whatsapp is also one of the most popular apps in the Netherlands and has millions of Dutch users. In fact, the app is now so well-known that the verb 'whatsappen' ('to whatsapp') was added to the Van Dale standard dictionary of the Dutch language in October 2012.

Applicable law and authorisation
Because the app is being used to process personal data on smartphones in the Netherlands, the Dutch DPA is authorised to launch an investigation in pursuance of the Dutch Data Protection Act (hereinafter called the Wbp) [Wet bescherming persoonsgegevens]. This personal data includes the mobile phone numbers, unique customer and device identifiers and (where specified) the push IDs and the profile names of whatsapp users. In addition, WhatsApp also processes the mobile phone numbers of non-users that are listed in the address books of whatsapp users.

WhatsApp uses the smartphones of whatsapp users – by means of the app that has been installed on the devices – to process personal data for use with the app.

The Wbp is imperative law (as is Chapter 11 of the Dutch Telecommunications Act (Tw) [Telecommunicatiewet]), which means that its applicability cannot be excluded by WhatsApp by means of a unilateral declaration or the general conditions in contracts with the users.

Access to the address book
People who want to use whatsapp must allow the app to access their entire electronic address book, including the mobile phone numbers of contacts that are not using the app (except in the latest app version on an iPhone with iOS 6). Because WhatsApp does not obtain unambiguous

consent from non-users to process their personal data and does not have any other legal ground for processing that data, WhatsApp is acting in breach of the provisions of article 8 of the Wbp.

WhatsApp does not actually need to process all the mobile phone numbers in users' address books in order for them to whatsapp with each other. Because WhatsApp (except in the latest app version on an iPhone with iOS 6) does not allow users to choose whether they want to make their contacts available to WhatsApp − and, if so, which ones − many of the mobile phone numbers that WhatsApp collects from the address books are excessive. WhatsApp is therefore acting in breach of the provisions of article 11, first section, of the Wbp.

Retention period
WhatsApp stores the personal data of inactive users for one year. Because WhatsApp has not demonstrated that the data of inactive users needs to be stored for such a long time, WhatsApp is acting in breach of the provisions of article 10, first section, of the Wbp.

Security
At the start of the investigation, the Dutch DPA and the OPC identified two security shortcomings, namely when creating passwords and when sending messages.

At the start of the investigation, WhatsApp generated passwords using the hashed WiFi MAC address on iPhones and the hashed IMEI device number on other types of smartphones. This working method exposed whatsapp users to the risk that others could pirate their passwords and in that way use their accounts to send and read messages. For this reason, WhatsApp was acting in breach of the provisions of article 13 of the Wbp. In response to the Preliminary Findings report, WhatsApp adopted a new method to create passwords. In December 2012, WhatsApp launched new versions of the app, and started to force active users to switch to these latest versions. Users are forced because they can no longer use the older versions of the app. There are still risks for inactive users that do not update their app. After all, users only obtain a new password when they *actively* install a new update. WhatsApp has stated that it will address these risks for inactive users, but it has not specified any dates. Because WhatsApp is currently not using the new method for all accounts, with regard to these users WhatsApp is (still) acting in breach of the provisions of Article 13 of the Wbp.

When the Dutch DPA and the OPC started their investigation, Whatsapp was using the app to send messages unencrypted. This meant that others could intercept the message contents in readable format. In response to the investigation, WhatsApp now uses encryption. This means that it is no longer acting in breach of the provisions of article 13 of the Wbp in this respect.

Status messages
All whatsapp users can read the status messages of other whatsapp users, and even those of unknown users whose mobile phone numbers are listed in their address books. In response to the investigation by the Dutch DPA and the OPC, WhatsApp has supplemented the information that it provides to its users about the distribution of status messages. The OPC stresses that WhatsApp must build in extra safeguards to prevent the widespread distribution of potentially sensitive status information. Although there seems to be no formal breach of the Wbp with respect to this point, the Dutch DPA endorses the recommendation of the OPC that whenever

users of whatsapp change their status message, they should be warned about the risk associated with the distribution of that status message.

Announced measures

In response to the investigation by the Dutch DPA and the OPC, WhatsApp has announced that priorities on its product development agenda are: (i) addressing the password security of inactive users, (ii) the manual addition of contacts, (iii) retention periods and the information about them and (iv) the addition of a warning/pop-up about the distribution of status messages, when users are adapting their status message. Whatsapp did not specify any dates for these measures.

1. INTRODUCTION

Together with the Canadian regulator Office of the Privacy Commissioner of Canada (hereinafter called OPC), the Dutch Data Protection Authority (Dutch DPA) [College bescherming persoonsgegevens] has launched an investigation into the processing of personal data by WhatsApp Inc. (hereinafter called WhatsApp), the developer of the 'whatsapp' mobile communication application (app).[1]

WhatsApp was founded in 2009 and is based in California in the United States.[2] WhatsApp is the owner and controller of the www.whatsapp.com website, the whatsapp software and the whatsapp app.[3] WhatsApp has declared that it has no offices outside the US. WhatsApp has not appointed a representative in the Netherlands.[4]

The whatsapp app is a widely-used instant messaging app for smartphones. The app is designed as a free alternative to SMS and is available for a range of smartphones and operating systems, including Apple's iPhone, Microsoft's Windows Phone, Research in Motion's Blackberry, Nokia's Symbian and S40 and devices equipped with Google's Android operating system. Users can also use whatsapp to send and receive photographs, videos and audio files (MMS).

The whatsapp app for the iPhone can be purchased for a one-off fee of EUR 0.89[5] (0,79 when the investigation started). On other operating systems, the app is free of charge for the first year.[6] The app can be used to send and receive messages free of charge. Users pay only the costs of data use over the Internet.

The app is very popular worldwide and is one of the world's top five best-selling apps. According to WhatsApp, since October 2011 more than a billion messages have been sent through the app every day.[7]

Whatsapp is also one of the most popular apps[8] in the Netherlands and has millions of Dutch users[9]. In fact, the app is now so well-known that the verb 'whatsappen' ('to whatsapp') was added to the Van Dale standard dictionary of the Dutch language in October 2012.[10]

---

[1] URL: http://www.whatsapp.com/.
[2] 3561 Homestead Road, Unit 16, Santa Clara, California 95010-5161.
[3] URL: http://www.whatsapp.com/legal/.
[4] Whatsapp's response on 17 May 2012 following a request for information, p. 2.
[5] URL: https://itunes.apple.com/nl/app/whatsapp-messenger/id310633997.
[6] See for example. URL: https://play.google.com/store/apps/details?id=com.whatsapp&hl=nl; http://www.windowsphone.com/nl-nl/store/app/whatsapp/218a0ebb-1585-4c7e-a9ec-054cf4569a79.
[7] URL: http://blog.whatsapp.com/index.php/2011/10/one-billion-messages/.
[8] URL: http://www.intelligence-group.nl/nl/actueel/augustus-2012/nieuws/facebook-en-whatsapp-meest-populaire-apps-onder-nederlandse-beroepsbevolking.
[9] Whatsapp's response on 17 May 2012 following a request for information, p. 3. [CONFIDENTIAL: (...)].
[10] 'Whatsappen opgenomen in Van Dale', *Nu.nl* 19 September 2012. URL: http://www.nu.nl/internet/2913592/whatsappen-opgenomen-in-van-dale.html. See also ''Whatsappen' als werkwoord in Dikke Van Dale', *Whatsappen.nl* 19 September 2012, updated on 17 October 2012. URL: http://www.whatsappen.nl/nieuws/2012/09/19/whatsappen-in-grote-of-dikke-van-dale/.

Research questions
The investigation concentrated on the following questions:

- Are the data that WhatsApp collects for the app personal data as defined in article 1, heading and under a, of the Dutch Data Protection Act (Wbp)?
- Does WhatsApp have a legal ground for processing the mobile phone numbers of non-users listed in the address books of whatsapp users as stipulated in article 8 of the Wbp?
- Does WhatsApp have a legal ground for processing status messages as stipulated in article 8 of the Wbp?
- Is it necessary for WhatsApp to collect all mobile phone numbers from the address books of whatsapp users and then process them (article 11, first section, of the Wbp: excessive use)?
- Are the data of whatsapp users stored for longer than is necessary for realising the purposes for which they are collected or subsequently processed (article 10 of the Wbp)?
- Has WhatsApp taken appropriate technical and organisational measures to protect personal data, for example, against the unauthorised cognizance of messages sent using the app as stipulated in article 13 of the Wbp?

Progress of the investigation
Prior to the investigation, the Dutch DPA and the OPC signed a *Memorandum of Understanding* (hereinafter called the MoU) regarding the mutual exchange of investigation data. This agreement came into effect on 16 January 2012. During the investigation, the Dutch DPA and the OPC shared investigation data as part of the MoU.[11]

In a letter dated 16 February 2012, the Dutch DPA notified WhatsApp in writing that it was launching an investigation into the processing of personal data in the framework of the app and requested information. WhatsApp replied by letter on 22 March 2012.

In a letter dated 9 May 2012, the Dutch DPA requested more detailed information. On 17 May 2012, WhatsApp supplied the requested information in a letter to the Dutch DPA.

In March and August 2012, the Dutch DPA conducted a digital investigation into the app.[12] The privacy policy[13] and the conditions[14] were forensically recorded. The app was installed on smartphones[15] registered to the Dutch DPA, and photographs/screenshots were made of the installation process and the user options of the app. Messages were exchanged between the

[11] Pursuant to article 2:5 of the General Administrative Law Act (Awb) [Algemene wet bestuursrecht], everybody involved in performing the activities of the Dutch DPA may make confidential data public insofar as this is necessary for the proper implementation of their administrative task.
[12] Pursuant to article 5:18 of the Awb, supervisory authorities are authorised, amongst other things, to investigate items (such as smartphones, for example) and to subject them to recordings (including making photographs/screenshots). See *Tekst & Commentaar AWB*: note 3B to article 5:18 of the Awb.
[13] URL: http://www.whatsapp.com/legal/#Privacy.
[14] URL: http://www.whatsapp.com/legal/#TOS.
[15] The app was installed on three smartphones with the operating systems: Android, iOS and Windows. The app was not tested on Nokia and BlackBerry.

smartphones, and the security of the message traffic was analysed using packet analysis software.[16]

The Dutch DPA sent its Preliminary Findings report of 2 October 2012 to WhatsApp on 15 October 2012, simultaneously with the preliminary findings of the OPC. An informal English translation was appended to the Preliminary Findings report. The Dutch DPA gave WhatsApp the opportunity to voice its view of the report.

In an email dated 30 October 2012, WhatsApp asked for a postponement of the deadline for giving its view. In an email dated 31 October 2012, the OPC, also on behalf of the Dutch DPA, notified WhatsApp that it would be granted a postponement up to and including 30 November 2012. In an email dated 29 November 2012, WhatsApp gave its view of the Preliminary Findings report.

On 4 and 5 December 2012, in consultation with the Dutch DPA the OPC contacted WhatsApp's advocate-delegate (by email and by telephone) and requested a reaction to a problem reported in the media. WhatsApp provided an explanation by email on 7 December 2012. In an email of 10 December 2012, the OPC, in consultation with the Dutch DPA, posed additional questions to WhatsApp in response to its view, with a request to take part, in the short term, in a video conference call to discuss that subject. In an email of 17 December 2012, WhatsApp reacted positively to the request. In emails of 18 December 2012, the OPC, in consultation with the Dutch DPA, explained the additional questions in more detail. In an email of 19 December 2012, WhatsApp sent two diagrams with detailed information. In an email of 20 December 2012, the OPC, in consultation with the Dutch DPA, asked for an explanation of the diagrams. WhatsApp provided an explanation in an email of 20 December 2012.

In December 2012 and January 2013, the Dutch DPA again conducted a digital investigation into the app. As part of the investigation, the password security was analysed and photographs/screenshots were taken of the installation process and the possible uses of the (latest versions of the) app.[17] On 4 January 2013, a conference call took place between the Dutch DPA, the OPC and WhatsApp and its advocate-delegate. In an email of 5 January 2013, the OPC, in consultation with the Dutch DPA, asked WhatsApp for further information. WhatsApp responded to this email in an email of 5 January 2013.

The Dutch DPA approved the Definitive Findings report on 15 January 2013.

WhatsApp's view
In its view (also in subsequent email correspondence and the conference call of 4 January 2013), WhatsApp states, in summary, that 'out-of-network' phone numbers (that is, numbers of non-users of the app) are disidentified and hashed on the whatsapp servers in a way that makes it extremely difficult for WhatsApp (or third parties) to recover the original numbers. WhatsApp states that to this extent it believed this (already) involves a compare and forget system.[18]

---

[16] URL: https://www.wireshark.org/.
[17] It relates to the whatsapp versions 2.8.9108 for Android, launched on 8 December 2012, 2.8.7 for iOS, launched on 7 December 2012 and 2.8.10.0 for Windows, launched on 19 December 2012.
[18] WhatsApp's view of 29 november 2012, p. 1.

With respect to the automatic generation of the password, WhatsApp states that it has adapted its working method in the sense that there are now app updates available that no longer use the WiFi MAC address or the IMEI device number and instead use [CONFIDENTIAL: (...)].[19]

Furthermore, WhatsApp points out that in the latest iOS version of the app (according to WhatsApp, the most commonly used operating system for the app), users have the option of refusing WhatsApp access to their electronic address book. If, in a dialog box displayed by the operating system, users refuse WhatsApp access to their address books, they can still enter a phone number manually in order to send that person a whatsapp message. With respect to access to the address book on smartphones with other operating systems, WhatsApp states that it sees no added value in developing a request for permission in the app itself.[20] According to WhatsApp, by installing the app users have granted WhatsApp permission to access their address books.[21]

In its view, WhatsApp indicates that it is busy identifying potential candidates that it can appoint as its representative in the Netherlands.[22]

WhatsApp stores the data of inactive users (for example, users that have installed whatsapp (once-off) free of charge, tried it out and then stopped using it) for one year. According to WhatsApp. it must store the data − particularly when it involves a paid account − for the subscription period to ensure good service with no loss of quality (unless it involves data deleted by the user before the expiry date). [23]

In its view, WhatsApp states that the addition of a warning/pop-up about the distribution of status messages − when users are adapting their status message – is now a priority on its product development agenda. [24]

Lastly, WhatsApp writes that it intends in a general sense to start working on retention periods and the information related to them.[25]

This report includes the business content of WhatsApp's view, section by section, with the Dutch DPA's reaction to it and information about whether the reaction has led to a change in the findings and related change(s) in the conclusions.

[19] Idem, p. 2.
[20] WhatsApp's email to the OPC on 4 January 2013.
[21] Idem.
[22] WhatsApp's view of 29 November 2012, p. 2.
[23] Idem.
[24] Idem.
[25] Idem, p. 3.

2. FINDINGS

2.1 Installing and using whatsapp

Anyone can download the whatsapp app from a number of different online app stores. Whatsapp for the iPhone can be purchased for a one-off fee of EUR 0.89 (at the start of the investigation: 0.79). On other operating systems, the app is free for a trial period of one year. The app can be used to send and receive messages free of charge. Users pay only the costs of data use over the Internet.

The app is accessible to and (partly) aimed at people living in the Netherlands. This assertion is supported by the fact that WhatsApp has published its frequently asked questions (FAQ) and various dialog boxes and screen settings in Dutch.[26] In addition, the standard text for inviting new users is in Dutch.

Figure 1 Standard text in Dutch for inviting new users

WhatsApp also makes the following specific appeal to Dutch translators:

Help translate whatsapp today! We're looking for translators in: Arabic, Danish, Dutch, Farsi, Filipino, Finnish, French, German, Hebrew, Hindi, Hungarian, Indonesian, Italian, Japanese, Korean, Malay, Norwegian, Polish, Portuguese (Brazil), Russian, Simplified Chinese, Spanish, Swedish, Thai, Traditional Chinese, Turkish, Urdu and many more languages.[27]

After downloading the app, the user must install it. The user is asked to allow the app to access various smartphone system help programs, such as read and write access (hereinafter called access) to the address book, internet access for creating network sockets, the exact (GPS) location, and writing to microSD storage, but also to functions such as 'Record audio', 'Send SMS messages', 'Call telephone numbers directly' and 'Launch automatically during start-up'.[28]

After installation, the user must use his smartphone to register with WhatsApp.

---

[26] URL: http://www.whatsapp.com/faq/?l=nl. During the investigation, the Dutch DPA verified that the telephone verification procedure also takes place in the Netherlands if SMS authentication fails.
[27] URL: http://translate.whatsapp.com/.
[28] The question whether access to system help programs other than read and write access to the address is lawful was not investigated by the Dutch DPA. Access to those other system help programs by the app on the smartphone is outside the scope of this investigation.

During the registration process, the user is first requested to read and accept the company's general conditions and privacy policy (hereinafter jointly called 'the conditions').

Once the user has read and accepted the conditions, he is asked to specify his country of residence and mobile phone number. In some cases, the app asks for the name that the user has defined for push notifications (used in iPhones and Windows Phones).

After the user has entered his country code and mobile phone number, WhatsApp collects the following data from the smartphone: the unique customer number (IMSI), the mobile phone number (MSISDN), the mobile country code (MCC) and the mobile network code (MNC). The unique IMSI customer number, the mobile country code and the mobile network code are stored for thirty days after the account has been created.[29]

WhatsApp automatically creates a user ID and password for users. The user ID is [CONFIDENTIAL: (...)], while at the start of the investigation the password was based on the unique 15-figure device number (IMEI). On the iPhone, the company used different data to generate the password: the iPhone's WiFi MAC address.[30] In response to the Preliminary Findings report, WhatsApp has changed the working method that it used to create passwords. In principle, app updates no longer use the WiFi MAC address or the IMEI device number and now use [CONFIDENTIAL: (...)] (see section 2.4.1).

WhatsApp then sends a regular SMS message with an activation code to the specified mobile phone number. In particular cases, the user can decide to be called by a voice recognition computer, which then reads out the activation code. The user should then enter the three-figure or six-figure activation code in order to verify the telephone number. The company uses the user's confirmation to check whether the data supplied by the user corresponds with the data that WhatsApp collected from the smartphone.

After this check, the user can choose an optional profile name. This name is not the whatsapp user ID. The chosen name is used as the sender name in messages sent by the user. Lastly, the user is registered and can start using whatsapp.

[29] Whatsapp's response on 17 May 2012 following a request for information, p.1.
[30] A MAC address is a unique number that the manufacturer records in equipment hardware − in this case in the inbuilt WiFi network card in the smartphone. MAC stands for *Medium Access Control*.

2.2 Access to the address book on the smartphone

During the installation process, WhatsApp asks if it can access the user's address book.[31] As soon as the user has installed the app, the mobile phone numbers of all contacts in the address book on the smartphone are uploaded to the whatsapp servers.

At the start of the investigation, it was not possible to install the app without allowing WhatsApp to access the full address book.[32] Nor was it possible to select individual contacts, even though other widely-used communication programs (including chat message services) did and do allow this.

If the address book is empty, the user is asked to invite friends by means of a standard SMS or email (see Figure 2).

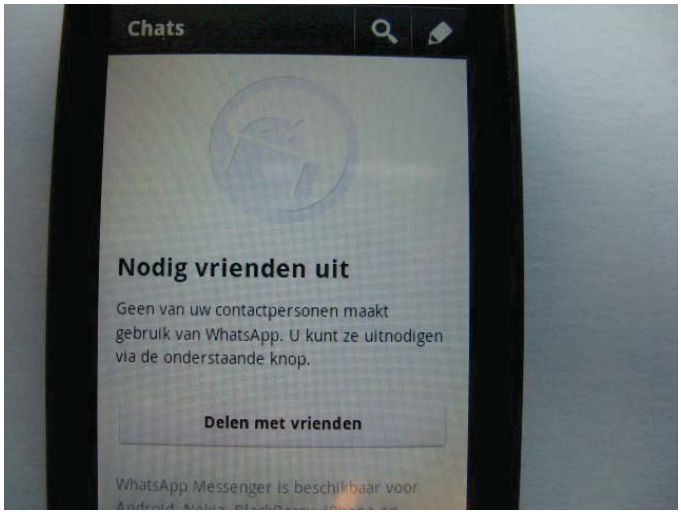

Figure 2 Screen displayed in Android if none of the contacts in the address book is a whatsapp user

During the installation process on the iPhone, at first it seemed to be possible to install the app without granting access to the address book. In the first dialog box, the user could still choose the option 'Do not allow'. However, in a later dialog box for saving 'Favourites' (preferred contacts with which the user wants to whatsapp), WhatsApp again requested access to the address book. Because this screen only contained the 'Allow' button and no option to close the screen, in reality the user could not refuse access to his address book (see Figure 3).

[31] In technical terms, the operating system requests authorisation before the app is installed − that is, on smartphones with the Windows and Android operating system. On these smartphones, no separate request for permission to access the address book is displayed in the app itself.
[32] In September 2012, The Dutch DPA has verified this for Android version 2.8.4771, for iPhone version 2.8.4 and for Windows Phone version 2.8.2.0.

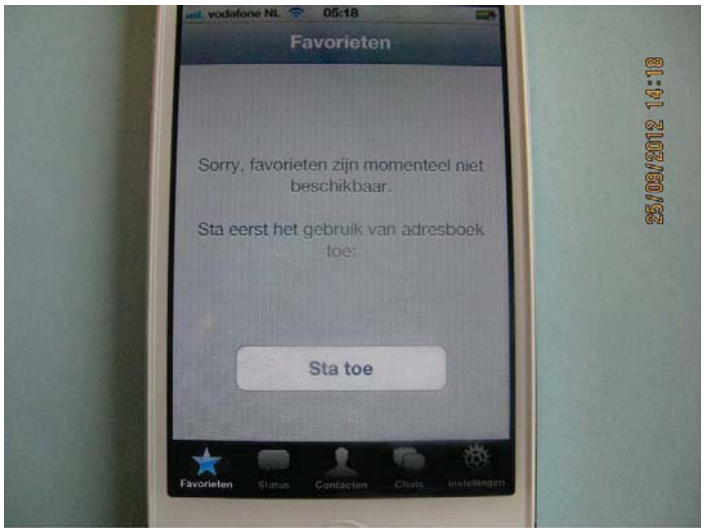

Figure 3 Dialog screen for mandatory access to the address book on the iPhone

In response to the Preliminary Findings report, WhatsApp stated that in the latest iOS version of the app (according to WhatsApp, the most commonly used operating system for the app), the user does have the option (i) to refuse WhatsApp access to his address book and (ii) to enter a phone number himself in order to send a whatsapp message. WhatsApp later stated that it saw no added value in developing a request for permission in the app itself on smartphones with operating systems other than iOS.[33] According to WhatsApp, by installing the app users automatically grant WhatsApp permission to access their address books.[34]

In early January 2013, the Dutch DPA confirmed that on iPhones with version 6 of the iOS operating system users can indeed install the app and use it without granting WhatsApp access to the address book. The dialog screen used during the installation process to request access to the address book includes both 'Refuse' and 'OK' buttons.[35]

[33] WhatsApp's email of 4 January 2013 to the OPC.
[34] Idem.
[35] The Dutch DPA checked and determined this for whatsapp version 2.8.7. on an iPhone with the iOS 6.0.1 operating system.

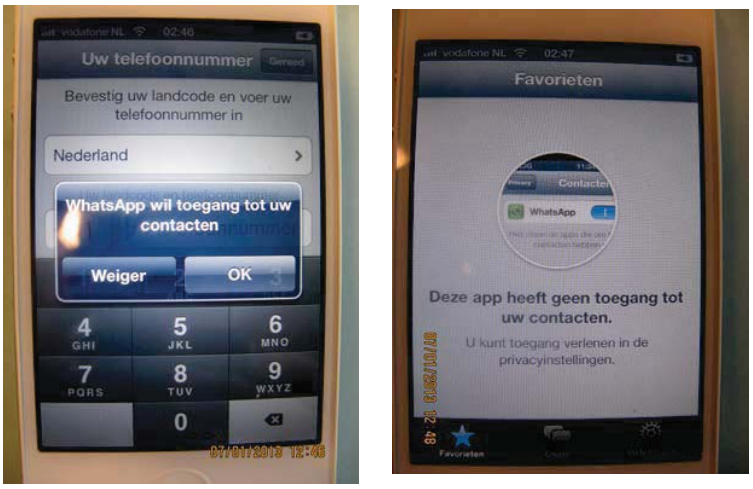

Figure 4 Dialog screens for optional access to address book on the iPhone

When the user refuses access to his address book, he can (still) use the app by entering a phone number to send a message to another whatsapp user and/or send an invitation to new contacts.

WhatsApp has declared that the address book is sent to the servers [CONFIDENTIAL: (...)], or at the moment that the user manually transmits a change in his address book to WhatsApp (refresh).[36] WhatsApp does this to show the user which of his contacts has decided to use whatsapp after all.[37]

WhatsApp has stated that it only collects the mobile phone numbers from the address book, but not other data such as names, email addresses, address data or other information.[38]

On the servers, the mobile phone numbers are marked as 'in-network' or 'out-of-network'. In-network telephone numbers are numbers of parties using whatsapp. Users can only send messages to other in-network numbers. Out-of-network telephone numbers are numbers of non-users of the app.

According to WhatsApp, in-network numbers are stored [CONFIDENTIAL: (...)] on the servers [CONFIDENTIAL: (...)]. Out-of-network numbers are stored with a cryptographic [CONFIDENTIAL: (...)] hash (unique hash value with a fixed length).[39] [CONFIDENTIAL: (...)]

---

[36] Whatsapp's response on 22 March 2012 following a request for information, p. 2. See also WhatsApp's View of 29 November 2012, p. 1

[37] WhatsApp's reaction to a request for information of 22 March 2012, p. 1.

[38] Idem.

[39] [CONFIDENTIAL: (...)] Hashing is a mathematical process that turns information (for example, text) into a unique hash code that is always the same length (for example, 128 bits). The size of the original text does not matter.

WhatsApp stated that it saves this data of non-users (out-of- network users) permanently in case they become whatsapp users at a later date.[40]

In response to the Preliminary Findings report, WhatsApp declared that out-of-network phone numbers are disidentified and hashed on the whatsapp servers in a way that makes it extremely difficult for WhatsApp (or third parties) to recover the original numbers. In an email of 20 December 2012, as explained in detail during the conference call of 4 January 2013, WhatsApp indicated how it calculates the hash of out-of-network numbers. [CONFIDENTIAL: (...)].[41][CONFIDENTIAL: (...)]

When a non-user decides to start using whatsapp, WhatsApp automatically adds that person's telephone number to the list of whatsapp users (in-network) on the smartphones of all the users that have this number in their address books, and to the in-network file on its own servers.

Every user can selectively block contacts with other whatsapp users.

2.3 Retention periods for the data of whatsapp users

WhatsApp has stated that the company does not save messages that have been delivered successfully. These messages are only stored on the smartphones of the senders and receivers of those messages.[42]

Messages saved on the whatsapp servers
Unsuccessfully delivered messages are stored on the servers for thirty days.[43] After delivery, these messages are automatically deleted from the servers. On the servers, the unsuccessfully delivered messages are stored [CONFIDENTIAL: (...)].

Messages saved on the smartphone
Users can delete data from their own smartphones, such as the messages they have exchanged with other users. Users can also choose to delete all sent and received messages from their smartphones. When they do this, however, the data is not yet definitively deleted. On Android smartphones, WhatsApp automatically creates a backup copy [CONFIDENTIAL: (...)].[44] On Nokia and Android smartphones, it is possible to restore recently deleted chats by de-installing the app and then re-installing it. During the (re-)installation, the backup is recognised and users are automatically asked whether the backup should be restored. Users with an iPhone can choose to make their own backups of particular data by synchronising with iTunes or iCloud.

[40] Idem.
[41] WhatsApp's email of 20 December 2012.
[42] WhatsApp's reaction in request for information of 22 March 2012, p. 2.
[43] Idem, p. 2.
[44] [CONFIDENTIAL: (...)]

Account data saved on the whatsapp servers[45]
Users can terminate their whatsapp accounts using the 'Delete account' option in the app's settings menu. WhatsApp has confirmed that a number of data items of such users are then immediately deleted from the whatsapp system. [46] This involves the following data:

- the user's mobile phone number is deleted from the whatsapp Favourites of other whatsapp users;
- the whatsapp user is deleted from all whatsapp groups;
- the message history is deleted from the smartphone.

WhatsApp has stated that it stores payment data for thirty days after users have terminated their accounts.[47] This data relates to the account type (free or paid), the user's telephone number and the termination/expiry date of the purchased service.[48] WhatsApp says that the reason for this retention period is that it makes it easier for users to re-register, for example, if users change their minds about terminating their account.

If a user no longer uses his account but does not terminate it, WhatsApp retains the user's data for one year.[49] This applies to users, for example, who have used the app (on smartphones other than the iPhone) free of charge for a year. If they do not pay for the app after that first year has elapsed, their data is still kept for one year. This retention period also applies, for example, to users that have changed their smartphone or mobile phone number but have not terminated their account.

In its view, WhatsApp takes the view that, particularly in the case of a paid account, it must store the data during the *subscription* period in order to provide a good service with no loss of quality (unless it involves data deleted by the user before the expiry date).[50]

---

[45] The scope of this investigation entails compliance with Article 10 of the Wbp (retention period) as far as it concerns the account data of inactive users.
[46] Whatsapp's response on 17 May 2012 following a request for information, p. 2
[47] Idem.
[48] The Dutch DPA has no evidence that WhatsApp collects and processes other types of payment data, such as credit card numbers, etc.
[49] WhatsApp's response on 17 May 2012 following a request for information, p. 2.
[50] WhatsApp's view of 29 November 2012, p. 2.

2.4 Security

2.4.1 Automatic password generation

WhatsApp automatically creates a user ID and password for users. The user ID is [CONFIDENTIAL: (...)], while at the start of the investigation the password was based on the unique IMEI device number (see also section 2.1). In order to generate the password on the smartphone, the IMEI was [CONFIDENTIAL: (...)] converted [CONFIDENTIAL: (...)] to a unique hash value with a fixed length. [CONFIDENTIAL: (...)]

WhatsApp used a different method on the iPhone. There, the WiFi MAC address was used to [CONFIDENTIAL: (...)] generate a password. The [CONFIDENTIAL: (...)] hash value was calculated by [CONFIDENTIAL: (...)] MAC address [CONFIDENTIAL: (...)] hashing [CONFIDENTIAL: (...)].[51]

During the investigation, he Dutch DPA took note of security warnings about the creation of passwords.[52] At the start of the investigation, anybody could use the mobile phone number and a password created in this way to access a whatsapp user's messages and send messages in their name (for more information, see section 3.9) [CONFIDENTIAL: (...)]

In response to the Preliminary Findings report, WhatsApp stated that it has changed the working method it uses to create passwords in the sense that it launched updates of the app in December 2012 that in principle no longer use the WiFi MAC address or the IMEI device number but rather [CONFIDENTIAL: (...)].[53] [CONFIDENTIAL: (...)]

In the case of active users, WhatsApp forces them to use the latest versions. Ussers are forced because they can no longer use the old(er) versions of whatsapp. [54] WhatsApp has said that it expects all active users to have switched to the latest versions of the app by mid-February 2013.[55] However, inactive whatsapp users (for example, users that install whatsapp (once-off) free of charge, try it out and then stop using it) have not been confronted with this 'forced update'.

In December 2012, the Dutch DPA analysed the password security and, after a digital investigation of the smartphones on behalf of the Dutch DPA, determined that WhatsApp has indeed changed the password security.[56] The Dutch DPA also determined that for the expired versions of inactive users whatsapp messages could (still) be intercepted and read using the

---

[51] [CONFIDENTIAL: (...)].
[52] 'WhatsApp accounts almost completely unprotected', *h-online.com* 14 September 2012. URL: http://www.h-online.com/security/news/item/WhatsApp-accounts-almost-completely-unprotected-1708545.html.
[53] WhatsApp's view of 29 November 2012, p.2.
[54] The CBP determined this for Android 2.8.9108 and Windows Phone version 2.8.10. iPhone version 2.8.4 has since also expired.
[55] WhatsApp statement made during the conference call of 4 January 2013.
[56] The CBP checked this for Android version 2.8.4771, for iPhone version 2.8.4 and for Windows Phone version 2.8.2.0.

[CONFIDENTIAL: (...)] (reproduced) password (based on the WiFi MAC address or the IMEI device number).[57]

During the conference call of 4 January 2013, WhatsApp acknowledged that there is still a risk for inactive users, and said that finding a remedy for this risk is now a priority on its product development agenda, but it did not specify a date.

2.4.2 Security of data transfer over the Internet

In early 2012, the Dutch DPA became aware of security warnings about problems related to the transfer of data over the Internet. Failure to encrypt the data transfer over the Internet could enable unauthorised persons to access mobile phone numbers and message content.[58]

At the start of the investigation, the OPC ascertained, using network analysis software, that no encryption was used on messages sent with the app.[59] That made it possible for others to intercept and read messages if the user was transmitting data over a public WiFi network.

In response to the research questions of the Dutch DPA and the OPC about the security measures that were taken, WhatsApp stated that it had introduced (new) end-to-end encryption and has been encrypting the content of messages since May 2012.[60] To make this possible, the company developed new software for all the smartphone types for which the app is available.

The Dutch DPA has confirmed that since mid-May 2012 all messages sent using the app are being encrypted.[61]

2.5 Status messages

A status message is a message with a maximum of 139 characters that enables users to display their status. Examples of status messages include 'available' or 'busy'. The app automatically provides every user with a status message that is visible to all other whatsapp users who have the user's mobile phone number in their address books. A user can suppress the automatic transmission of the status message to individual whatsapp users by adding those other whatsapp users to a block list, but that list can only contain people whose mobile phone numbers he knows. Moreover, his telephone number may be listed in the address books of many other whatsapp users whom he does not know.[62]

---

[57] Idem.
[58] See, for example, the warning of Secunia, an international IT security company specialising in vulnerability management (identifying shortcomings in the security of software) and with its registered offices in Copenhagen, Denmark. URL: https://secunia.com/advisories/product/39212/.
[59] On 13 January 2012, using packet analysis software the OPC verified that the messages were sent and received in readable format.
[60] Whatsapp's response on 17 May 2012 following a request for information, p. 2.
[61] The Dutch DPA checked the following software versions: Android version 2.8.1504, iOS version 2.8.2, Windows Phone version 2.8.00.
[62] Whatsapp conditions of 7 July 2012, section 5 under A. URL: http://www.whatsapp.com/legal/ (URL visited on 26 September 2012 and 3 January 2013).

The standard setting for status messages is: '*Hey there! I am using WhatsApp'* (see Figure 5). Users can use the app menu to change this message. The status menu contains a number of standard options, but users can also enter their own text to create a personalised status message. These types of user-defined status messages can also involve sensitive data, such as the user's exact location, or information about his health.

Users can re-activate the standard message by manually re-entering the standard text. Once a text has been entered, it can always be accessed through the menu. This means that users can use the menu to re-activate the standard message if they so wish. It is only on the iPhone that the status can be deleted with a separate button (and therefore remains empty).

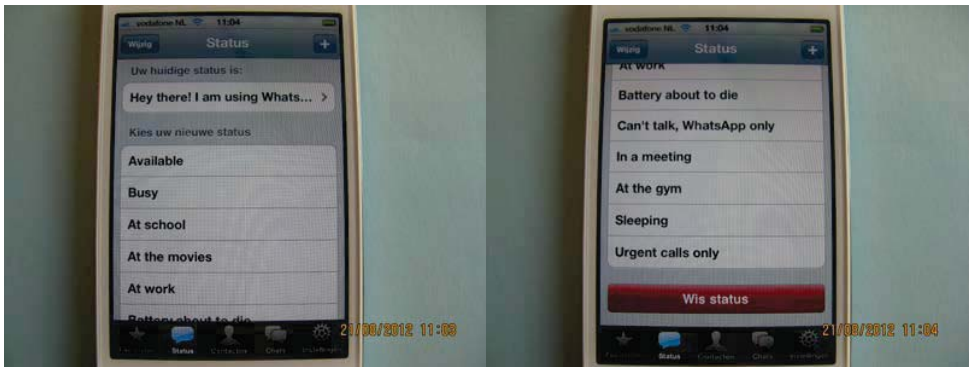

Figure 5 Dialog screen for status messages

The conditions of 5 January 2012 contained a separate section[63] about status messages ('*User Status Submissions*'). In response to the investigation conducted by the Dutch DPA and the OPC, WhatsApp has expanded this section. Users are now informed that their status is shared with all other users of the app whose mobile phone numbers are listed in their address books. This information has been added to the conditions of use of 7 July 2012.[64]

---

[63] On 5 January 2012, section 5 under A contained the text: '*The WhatsApp Service permits the submission of status text and other communications submitted by you and other users ("User Status Submissions") and the hosting, sharing, and/or publishing of such User Status Submissions. As clarified in the following section, you retain your ownership rights in your User Status Submissions. You understand that whether or not such User Status Submissions are published, WhatsApp does not guarantee any confidentiality with respect to any submissions.'*

[64] The text in Section 5 under A, which has been revised since 7 July 2012, reads as follows: '*The WhatsApp Service allows WhatsApp users to submit status text, profile photos and other communications submitted by you, as well as the automatic submission of your "last seen" status (collectively, the "Status Submissions"). These Status Submissions may be hosted, shared, and/or published as part of the WhatsApp Service, and may be visible to other users of the Service who have your mobile phone number in their mobile phone and which you have not expressly blocked. For clarity, direct messages, location data and photos or files that you send directly to other WhatsApp users will only be viewable by those WhatsApp user(s) or group(s) you directly send such information; but Status Submissions may be globally viewed by WhatsApp users that have your mobile phone number on their smartphone, unless the user is blocked by you. Currently, we have no method or providing different levels of visibility of your Status Submissions among users that have your mobile phone number – you acknowledge and agree that any Status Submissions may be globally viewed by users that have your mobile phone number, so don't submit or post status messages or profile photos that you don't want*

In its view, WhatsApp states that the addition of a warning/pop-up about the distribution of status messages − when users are adapting their status message – is now a priority on its product development agenda.[65]

3 ELABORATION OF THE LEGAL FRAMEWORK AND ASSESSMENT

3.1 Applicable law

Elaboration of the legal framework
Pursuant to Article 4, first and second sections, of the Dutch Data Protection Act (Wbp), the Act is applicable to the processing of personal data (a) in the context of the activities of a branch office in the Netherlands belonging to a controller or (b) by or on behalf of a controller with no branch office in the EU, using automated or non-automated means in the Netherlands, unless these means are only used to transfer personal data. This article is an implementation of Article 4 of European Privacy Directive 95/46/EC (hereinafter called the Privacy Directive).

Consideration 20 in the Privacy Directive reads: '*Whereas the fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive; whereas in these cases, the processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice.'*

The term 'means used' in consideration 20 of the Privacy Directive implies (i) an activity practiced by the controller and (ii) the intention to process personal data.[66]

The term 'means'[67] includes human and/or technical means. This also includes the collection of personal data by means of the computers of users, for example with cookies or JavaScript, or by means of smartphones of customers using specific software that has been installed on the smartphones.[68] The party responsible for the processing does not have to own or be in possession of the means in order for the processing to be within the scope of the Wbp.[69]

---

to be seen globally. A good rule of thumb is if you don't want the whole world to know something or see something, don't submit it as a Status Submission to the Service.' URL: http://www.whatsapp.com/legal/ (URL visited on 26 September 2012 and 2 January 2013).

[65] WhatsApp's view of 29 November 2012, p. 2.

[66] WP29 Advisory view 8/2010 on applicable law, p. 20 and WP29 Working document on the international application of the EU's data protection legislation to the processing of personal data on the Internet by websites from outside the EU of 30 May 2002, p. 9. URL: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_en.pdf and http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp56_en.pdf.

[67] For the term 'equipment' in the English-language version of the Privacy Directive, in other EU languages − such as Dutch − the word 'means' is used. This makes the case for a broad interpretation of the term. WP29 Advisory view 8/2010 on applicable law, p. 8.

[68] Idem, p. 21. See also WP29 Working document on the international application of the EU's data protection legislation on the processing of personal data on the Internet by websites outside the EU of 30 May 2002, p, 11 ff.

[69] See in the same sentence in WP29 Advisory view 8/2010 on applicable law, p. 20.

Directive 2002/58/EG on privacy and electronic communication (the e-Privacy Directive) regulates the protection of personal data and the privacy of the users of public electronic communication services. The provisions in the e-Privacy Directive (implemented in the Dutch Telecommunications Act [Telecommunicatiewet]; hereinafter called the Tw) give a more detailed interpretation to particular general standards in the general Privacy Directive, which are implemented in the Wbp (for example, further limitation/restriction of the permitted processing). This is not a situation involving a *lex specialis* – that is, a special law that overrides a general law.[70]

Assessment
WhatsApp, based in California and with no registered offices outside the United States, uses the smartphones of whatsapp users – by means of the app that has been installed on the devices – as a means of processing personal data in the context of the app (for more information, see section 3.5 of this report).

The app can be accessed by people in the Netherlands, and the service is also (partly) aimed at people in the Netherlands. This is evident, amongst other things, from the fact that WhatsApp displays various dialog boxes and (settings) screens (including the standard text for inviting new contacts) and the frequently asked questions (FAQ) in Dutch (see section 2.1 of this report). Furthermore, WhatsApp appeals to Dutch translators to help it provide (further) information in Dutch.[71]

In view of the above, the Wbp applies to the processing of personal data by WhatsApp in the context of the app (as further limited/restricted by the Tw, insofar as this is relevant for this investigation; for more information, see section 3.6 of this report).

The Wbp is imperative law (as is Chapter 11 of the Tw). This means that its applicability cannot be excluded by a unilateral declaration or contractually in WhatsApp's general provisions.[72]

---

[70] See, amongst others, *Parliamentary documents II* 1999/2000, 26 410, no. 7, p. 2*: 'In general, it cannot be stated that special legislation prevails over the more general privacy regulations. This adage* [namely: the rule 'lex specialis derogat legi generali'; added by the Dutch DPA] *only applies in those cases where the special law has an exclusive effect in relation to the Wbp – that is, that it contains an exhaustive regulation compared to which the Wbp no longer applies. A summary of this type of specific legislation is contained in Article 2 of the Wbp. In those cases where the specific legislation is not within the scope of this Article 2, the «special law supersedes general law» adage does not, however, apply. After all, in these cases the Wbp is applicable alongside the specific legislation. In that case, the Wbp therefore has a supplementary effect, namely for those components not covered by the special legislation. The 1997 Social Security (Organisation) Act and the Telecommunications Act are examples of this. (…)',* [underscore added by the Dutch DPA].
[71] URL: http://translate.whatsapp.com/.
[72] *Parliamentary documents II* 1997/1998, 25 892, no. 3, p. 10: '[It, addition by the Dutch DPA] *(…) is assumed that personal rights are in principle non-transferable and therefore not subject to contractual waiver. Based on this general notion, the regulations in the Wbp apply as imperative law.'* Whatsapp's Terms of Service and Privacy Notice, which are only available in English, state: '*You agree that: (i) the Whatsapp Service shall be deemed solely based in California; (ii) the Whatsapp Service shall be deemed a passive server that does not give rise to personal jurisdiction over Whatsapp, either specific or general, in jurisdictions other than California; and (iii) that you agree to subject to the jurisdiction of California in the event of any legal*

3.2 Jurisdiction of the Dutch DPA

Elaboration of the legal framework
Pursuant to Article 61, first section, in conjunction with Article 51, first section, of the Wbp, the task of the Dutch DPA, as a supervisory authority, is to regulate (that is, it has jurisdiction with regard to) the processing of personal data in accordance with the provisions specified in and pursuant to the law.

Assessment
In this way, the Dutch DPA supervises compliance with the provisions of the Wbp and (insofar as is relevant to this investigation) of Chapter 11 of the Tw insofar as it involves the processing of personal data in the electronic communication sector.[73] The jurisdiction for launching an investigation is derived from Article 60, first section, of the Wbp.

On the basis of Article 60, first section, of the Wbp, the Dutch DPA, in its official capacity, or at the request of an interested party, can launch an investigation into the way the provisions specified in and pursuant to the law are applied to data processing.

In view of the above (section 3.1 and section 3.2), the Dutch DPA has jurisdiction (that is, it is authorised as the supervisory authority) with regard to the processing of personal data in the context of the app by WhatsApp.

3.3 Controller

Elaboration of the legal framework
On the basis of Article 1, heading and under d, of the Wbp[74], the controller is the natural person, legal entity or any other administrative body, which, either alone or together with others, determines the objective and means of processing personal data.

---

dispute. These Terms of Service shall be governed by the internal substantive laws of the State of California, without respect to its conflict of laws principles. Any claim or dispute between you and Whatsapp that arises in whole or in part from the Whatsapp Service shall be decided exclusively by a court of competent jurisdiction located in Santa Clara County, California'. And: '*Special Note to International Users The WhatsApp Site and Service are hosted in the United States and are intended for and directed to users in the United States. If you are a user accessing the WhatsApp Site and Service from the European Union, Asia, or any other region with laws or regulations governing personal data collection, use, and disclosure, that differ from United States laws, please be advised that through your continued use of the WhatsApp Site and Service, which are governed by California law, this Privacy Policy, and our Terms of Service, you are transferring your personal information to the United States and you expressly consent to that transfer and consent to be governed by California law for these purposes.'* URL: http://www.whatsapp.com/legal/?l=nl.

[73] *Parliamentary documents II* 2002/03, 28 851, no. 7, p. 53-54.

[74] This article is an implementation of Article 2, under d, of the Privacy Directive.

Assessment
WhatsApp, based in California in the United States, determines the purposes of and the means used for processing personal data in the context of the app.[75] WhatsApp is therefore the controller of the processing of personal data in the context of the app.

3.4 Representative in the Netherlands

Elaboration of the legal framework
On the basis of Article 4, third section, of the Wbp[76] a controller without a branch office in the EU is prohibited from processing personal data unless that controller appoints a person or body in the Netherlands that acts on its behalf in accordance with the provisions of the Wbp. This article requires controllers outside the EU to appoint a representative in the Netherlands that is liable for compliance with the law on Dutch territory.[77] For the application of the Wbp and the contributory provisions, the representative is regarded as the controller (Article 4, third section, second sentence, of the Wbp).

Assessment
WhatsApp has stated that it has no branch office in Europe and that it has not appointed a representative in the Netherlands. In response to the Preliminary Findings report, WhatsApp stated that it wants to appoint a representative in the Netherlands in the short term, but that it has not (yet) made that appointment. With respect to this point, therefore, WhatsApp's view will not lead a change in the conclusions in the report. WhatsApp is therefore still acting in breach of the provisions of Article 4, third section, of the Wbp.

3.5 Processing personal data

Elaboration of the legal framework
According to Article 1, heading and under a, of the Wbp, by a 'personal data item' is meant *every data item related to an identified or identifiable natural person*.

'Processing of personal data' is defined in Article 1, heading and under b, of the Wbp and includes collecting, recording, saving, using, combining and linking personal data.[78]

---

[75] See, for example: '*This is an agreement between WhatsApp Inc., a California corporation ("WhatsApp"), the owner and operator of www.whatsapp.com (the "WhatsApp Site"), the WhatsApp software, including WhatsApp Messenger (collectively, including all content provided by WhatsApp through WhatsApp Messenger and the WhatsApp Site, the "WhatsApp Service", or the "Service"), and you ("you" or "You"), a user of the Service.'* And: '*This Privacy Policy is part of WhatsApp's Terms of Service and covers the treatment of user information, including personally identifying information, obtained by WhatsApp, including information obtained when you access the WhatsApp Site, use the WhatsApp Service or any other software provided by WhatsApp.'* URL: http://www.whatsapp.com/legal/?l=nl.

[76] This article is an implementation of Article 4, second section, of the Privacy Directive.

[77] See *Parliamentary documents II* 1997/98, 25 892, no. 3, p. 76: '*Compliance with the statutory regulations for the processing, on Dutch territory, of personal data from outside the Union.'* See also WP29 Advisory view 8/2010 on applicable law, p. 23.

[78] Article 1, preamble and under b, of the Wbp understands – in full – 'processing of personal data' to be: '*every act or every entirety of acts related to personal data, including in any case collecting, recording,*

Article 1, heading and under a, of the Wbp is an implementation of Article 2, heading and under a, of the Privacy Directive:

> *'For the purposes of this Directive:*
> *"personal data" shall mean any information referring to an identified or identifiable natural person ("data subject"); an identifiable person is a person that 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.'*

All data that can provide information about an identifiable natural person must be regarded as personal data.[79]

Data are personal data when by their nature they relate[80] to a person, such as factual or valuating data about attributes, views or forms of behaviour or – in view of the context[81] in which it is being processed – contributes to the way the data subject is judged or treated in the public interest.[82] In the latter case, the use to which the data can be put contributes to answering the question whether this involves personal data.[83] In addition, data that does not relate directly to a particular person but to a product or a process, for example, can furnish information about a particular person and is in that case personal data.[84]

A person is identifiable if his identity can be determined, within reason[85], without disproportionate effort, directly or through further steps, by means of data that is so characteristic − in itself or in combination with other data − for that person[86]. In order to

---

sorting, saving, editing, modifying, retrieving, viewing, using, supplying data by forwarding or distributing it or making it available in any other way, combining, linking, as well as blocking, expunging or erasing data.'

[79] *Parliamentary documents II* 1997/98, 25 892, no. 3, p. 46.

[80] See WP29 Advisory view 4/2007 on the term 'personal data' of 20 June 2007, p. 10-11 and 25. URL: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf: '*Information "relates to" a person when it involves information "about" that person'* − in other words, the content. Idem, p. 10.

[81] Comp. idem, p. 10: Information 'relates to' a person '*when, taking account of all the circumstances of the exact case, data is being used or probably will be used with the aim of judging a person, treating a person in a particular way or influencing the status or the behaviour of that person'* − in other words, the goal.

[82] *Parliamentary documents II* 1997/98, 25 892, no. 3, p. 46. Comp. WP29 Advisory view 4/2007 on the term 'personal data' of 20 June 2007, p. 11: Information 'relates to' a person '*if its use, taking all the circumstances of the case into account, can be expected to have consequences for a person's rights or interests'* − in other words, the result.

[83] *Parliamentary documents II* 1997/98, 25 892, no. 3, p. 46. See also idem, p. 47: '*(…) Here, it is not relevant whether the intention to use the data for that objective is also present. A data item is already a personal data item when that data item can be used for a goal focussed on the person'*, [underscore added by the Dutch DPA].

[84] Idem, p. 46-47.

[85] Idem, p. 47-49. The legislative history of the Wbp contains the following remark on the term 'disproportionate effort': *'This would be the case, for example, if the identification of people by computer were to take many days.' Parliamentary documents II* 1998/99, 25 892, no. 13, p. 2.

[86] *Parliamentary documents II* 1997/98, 25 892, no. 3, p. 48. For example, '*cases (…) where data cannot be directly traced by name, yet the person can still be identified using the available means − for example, a number. This might include a situation in which a list of numbers and corresponding names is available, either through a*

determine whether a person is identifiable, it is necessary to examine all the means that it may be assumed can be used, within reason, by the controller or any other person to identify that person.[87] This assumption must be based on a reasonably equipped controller. [88] In concrete cases, however, it must be assumed that the controller has special expertise, technical facilities and the like at its disposal.[89]

Assessment
In sections 2.1 through 2.5 of this report, the Dutch DPA ascertained that WhatsApp has processed at least the following combinations of data related to/about whatsapp users in various devices and systems:

- mobile telephone number (MSISDN), including the country and network code;
- IMSI (unique customer number);
- (hashed) IMEI (unique device number);
- (hashed) MAC address of the iPhone (for whatsapp users with an iPhone);
- 'payment data', such as the account type (free trial or paid account), the mobile phone number and the end date of the free trial or paid account;
- content of SMS and MMS messages, including the ID for push messages: the name that whatsapp users have defined for push messages (for whatsapp users with an iPhone or Windows Phone) and the profile name (if and insofar as whatsapp users have specified a profile name);
- (personal) status messages.

In addition, WhatsApp processes the mobile phone numbers (including the country and network code) of non-users of the app services when they are listed in the address books of whatsapp users (hereinafter individually or jointly called: the data subjects).
In sections 2.1 through 2.5 of this report, the Dutch DPA ascertained that WhatsApp collects/generates the abovementioned data using the app installed on the smartphones of whatsapp users. With the exception of the content of successfully delivered messages and status messages, WhatsApp also records the abovementioned data on an individual personal level and saves it for a minimum of thirty days to a year.

Information 'about' a natural person

---

public source (such as the telephone directory), or through a source that can only be consulted by a particular category of people (for example, the vehicle registration database by the police or a bank account number by bank employees). The data linked to those numbers is – although not by name – personal data because of the available option to use the numbers to ascertain the identity of the people involved.' Parliamentary documents II 1998/99, 25 892, no. 13, p. 2.

[87] *Parliamentary documents II* 1997/98, 25 892, no. 3, p. 48. Here, all the relevant factors must be taken into account, such as the costs of identification, the intended objective of the processing, the way the processing is structured, the benefit expected by the party responsible for the processing, the interests at stake for the persons involved, the risk of organisational shortcomings (for example, breaches of the obligation to confidentiality) and technical malfunctions. WP29 Advisory view 4/2007 on the term 'personal data' of 20 June 2007, p. 15.

[88] *Parliamentary documents II* 1997/98, 25 892, no. 3, p. 48-49.

[89] Idem, p. 49.

As an example of personal data that does not relate directly to a particular person but to a product or a process, for example, the legislative history of the Wbp refers to the telephone number (here: the MSISDN, including country and network code).[90]

The mobile phone number, the unique IMSI customer number and, for existing users of the app until they start using the new password security, the (hashed) unique IMEI device number or the (hashed) MAC address of the iPhone (unique customer and device identifiers) in combination with the content-related communication data from sent and receive messages and status messages, including (if and insofar as they have been specified) the push ID and the profile name of a whatsapp user, and/or (technical) data about the use of the app are by their very nature also data related to the behaviour of a natural person (information about the person's communication behaviour using the app).[91]

Furthermore, the app use of a whatsapp user can provide clues, for example, about his interests, social background, income or family structure. Such information can be used for (direct) marketing and profiling purposes.[92] Whether it is WhatsApp's intention to use the data for either those purposes or other purposes is not of overriding importance. The data can already be regarded as personal data when it can be used for this type of intention aimed at the individual [93] and that possibility exists. As indicated above, WhatsApp has access to (data about) sent and received messages, (technical) data about the use of the app and contact data items (including the mobile phone number).

Identifiability of the person in question
For WhatsApp, these data items can be directly linked to each other or indirectly reduced to an identifiable natural person (a whatsapp user or a non-user of its app services).

As far as whatsapp users are concerned, WhatsApp has at least their mobile phone numbers at its disposal. WhatsApp also has the mobile phone numbers of non-users of its app service after the telephone numbers in the address books of whatsapp users have been synchronised. The

---

[90] Idem: '*In addition, (…) under certain circumstances telephone numbers (Data Inspection Board 8 July 1993, 93.A.002) should be regarded as a personal data item.'* And: *Parliamentary documents II* 1998/99, 25 892, no. 6, p. 27: '*Telephone numbers are not always personal data in the sense of the law – for example, not when they have been assigned to a legal entity or an administrative body and the number cannot be traced back to an individual natural person – for example, because that person is a permanent user.'* See also Court of Justice of the European Union 6 November 2003, case C-101/01 (*Lindqvist*), ground for a decision 27: '*(…) a reference to different people on an Internet page by name or otherwise – for example, with their telephone number or information about their work situation and their interests,* [can be, addition by the Dutch DPA] *regarded as the full or partial automated processing of personal data in the sense of Article 3, section 1, of Directive 95/46 (…).'* See also Court case Dordrecht 31 August 2004, *NBSTRAF* 2004, 422 on the GSM number (MSISDN) as personal data.
[91] In this way, information can be derived about the communication behaviour of the data subject and sometimes also the content of the communication.
[92] Definitive findings of the Investigation by the Dutch DPA into the collection of WiFi data with Street View cars by Google of 7 December 2010, p. 35 (z2010-00582). URL: http://www.cbpweb.nl/downloads_rapporten/rap_2011_google.pdf.
[93] *Parliamentary documents II* 1997/98, 25 892, no. 3, p. 47.

mobile phone number is a personal data item because it is a direct contact data item that anyone can use to identify a person directly or indirectly by taking intermediate steps.

In addition, WhatsApp also has at its disposal the unique IMSI customer number, the (hashed) unique IMEI device number or the (hashed) MAC address of the iPhone of whatsapp users. Without disproportionate effort, WhatsApp can link the data items to each other or, if necessary, take intermediate steps to trace the data subjects (for more information about the traceability of the (hashed) IMEI and MAC address, see section 3.9).

Identification is also possible without finding out the name of the data subject. All that is required is that the data can be used to distinguish one particular person from others. The view of the Article 29 Working party on the term 'personal data' includes the comment: '*(…) that although identification by means of the name is the most common method in practice, the name is not necessary in all cases to identify a person. This is the case when other means of identification are used to distinguish somebody from other people. In computer files that include personal data, the registered people are usually assigned a unique identification code to prevent people from being mixed up in the file. On the world wide web, using monitoring instruments for web traffic, it is a simple task to identify the behaviour of a machine and therefore also its user. (…) In other words, the identification of a person no longer requires the capacity to find out his or her name. The definition of the term "personal data item" also reflects this fact*', [underscores added by the Dutch DPA].[94]

When data is linked to a unique number, it generally refers to an individualised person. In that context, the Dutch DPA also refers to the consideration in the judgment of the European Court of Justice of 6 November 2003 that '*(…) the display of various people on an Internet page with their names or other data – for example, with their telephone numbers or information about their work situation and their interests, can be regarded as the full or partial automated processing of personal data in the sense of Article 3, section 1, of Directive 95/46.*'[95]

Hashing

Hashing can be used in different ways. Hashing is used, for example, to secure passwords stored in a database. It is possible to check whether an entered password is correct by comparing the hash value of the input with the hash value of the password already stored in the database. It is not necessary to know the password in order to perform this check. In particular cases and under particular conditions, the hashing of personal data, *in combination with* other measures and safeguards, leads to disidentification.[96] Whether disidentification occurs greatly depends on the actual circumstances of the case. In any case, disidentification by means hashing has not taken place if the original value can be recovered on the basis of a hash – for example, the hash can be calculated back to the original (identifying) data item or can be recalculated. This is the case, for example, when the controller has access to the hashing formula and the original data item.

In its view (also in subsequent email correspondence and the conference call of 4 January 2013), WhatsApp takes the viewpoint that 'out-of-network' phone numbers are disidentified and

[94] WP29 Advisory view 4/2007 on the term 'personal data' of 20 June 2007, p. 14.
[95] Court of Justice of the European Union 6 November 2003, case C-101/01 (*Lindqvist*), ground for a decision 27.
[96] In that context, for example, hashing can have added value as an *intermediate step* in a disidentification process.

hashed on the whatsapp servers in such a way that it is extremely difficult for WhatsApp (or third parties) to recover the original phone numbers.[97] In section 2.2 of this report, the Dutch DPA determined that WhatsApp can access the hashing formula [CONFIDENTIAL: (...)] and the original data item. That means that WhatsApp can recalculate the hashed out-of-network numbers without disproportionate effort and can create a lookup table, for example, of all out-of-network numbers in readable (plain text) and hashed format. Hashing has therefore not brought about disidentification. The same applies to the hashed unique IMEI device number or the hashed MAC address of the iPhone of whatsapp users. With respect to this point, therefore, WhatsApp's view does not lead to a change in the conclusions in the report that the hashed data can also be traced back to identifiable natural persons.

In view of the above, the data that WhatsApp processes is personal data in the sense of Article 1, under a, Wbp.

3.6 Legal ground

3.6.1 Processing the data of non-users listed in the address books of whatsapp users

Elaboration of the legal framework
In order to process personal data, a legal ground is required as enumerated in Article 8, heading and under a through f, of the Wbp.[98]

> Article 8, heading and under a and f, of the Wbp, stipulates, insofar as is relevant to this investigation:
> *Personal data may only be processed if:*
> *a. the data subject has granted his unambiguous consent for that data to be processed;*
> *(…)*
> *f. it is necessary to process the data to uphold the legitimate interests of the controller or of a third party to whom the data will be supplied, unless the interests or the fundamental rights and freedoms of the data subject, particularly the right to the protection of privacy, prevails.*

With regard to placing and transferring data onto and from the devices of users, Article 5, third section, of the e-Privacy Directive (implemented in Article 11.7a of the Tw (new)[99], which came into effect on 5 June 2012)[100], stipulates a more detailed limitation/restriction of the permitted processing/the legal ground as enumerated in Article 8 of the Wbp that may be taken into account.

> Article 11.7a, first section, of the Tw (new) reads:

---

[97] WhatsApp's view of 29 November 2012, p. 2.
[98] This article is an implementation of Article 7, heading and under a up to and including f, of the Privacy Directive.
[99] The legislative history of the Tw includes a remark about the scope of this provision: '*Because the provision has the aim of protecting users, this provision applies to all parties that wish to place data on the peripheral equipment of users in the Netherlands, or wish to read data stored on that equipment, regardless of where that party has its place of business.' Parliamentary documents I* 2011/12, 32 549, E, p. 7.
[100] Article VII, first section, of the Decree on the implementation of revised telecommunication directives (Staatsblad [*Bulletin of Acts and Decrees*] 2012, 236).

Without prejudice to the Protection of Personal Data Act, anybody who wishes to gain access by means of electronic communication networks to data stored in a user's peripheral equipment or wishes to save data in the user's peripheral equipment should:
a. provide the user with clear and comprehensive information in pursuance of the Protection of Personal Data Act, and in any case information about the purposes for which it wishes to gain access to the relevant data or for which it wishes to save the data, and
b. have obtained the user's consent for the relevant activity.

The provision in the first section does not apply insofar as it involves the technical storage of or access to data with the sole objective of enabling the information company to provide a service requested by the subscriber or user for which the storage of or access to data is strictly necessary (Article 11.7a, third section, of the Tw (new), insofar as relevant for this matter).

Consent from a user is defined in Article 11.1, heading and under g, of the Tw and includes consent in the sense of Article 1, heading and under i, of the Wbp.

There is only consent in the sense of Article 1, heading and under i, of the Wbp if it is 'free', 'specific' and 'informed'. 'Free' means that the data subject must be able to exercise his will in freedom.[101] 'Specific' means that the expression of will must relate to the processing of a particular data item or a limited category of data processing (no generally formulated authorisation).[102] 'Informed' means that the data subject must have the necessary information at his disposal in order to form an accurate judgement.[103]

'Unambiguous consent' means that the controller may not assume to have been granted consent just because the data subject has not remarked upon the data processing (or: 'consent' that is deemed to issue from the data subject's failure to act or to respond verbally).[104]

Assessment
During its digital investigation into the app, the Dutch DPA ascertained that during the installation process WhatsApp requests read and write access to the user's address book (see section 2.1 of this report). After the user has installed the app (except if a user with the latest app version on an iPhone with the iOS 6 operating system has refused WhatsApp access to his address book), WhatsApp transfers the mobile phone numbers from the user's address book to its own address book, including the numbers of non-users. WhatsApp uses this data, records it and saves it to enable users to whatsapp with each other − that is, to show the user which of his contacts are (or have started) using whatsapp.

---

[101] *Parliamentary documents II* 1997/98, 25 892, no. 3, p. 65.
[102] Idem. The view of the Article 29 Working party on the definition of 'consent' includes the following remark on this subject: '*General consent without a precise indication of the aim of the processing to which the data subject agrees does not comply with this requirement. That means that the information about the goal of the processing must not be included in the general provisions but in a separate consent clause.*' WP29 Advisory view 15/2011 on the definition of 'consent' of 13 July 2011, p. 34-35. URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/view-recommendation/files/2011/wp187_en.pdf.
[103] *Parliamentary documents II* 1997/98, 25 892, no. 3, p. 65.
[104] Idem, p. 66 and 67. See also WP29 Advisory view 15/2011 on the definition of 'consent' of 13 July 2011, p. 28 and 41.

In section 3.5 of this report, the Dutch DPA ascertained that the mobile phone numbers of non-users that are transferred from the address books of whatsapp users are personal data. In order to process the personal data of non-users in this way, in addition to consent as stipulated in Article 11.7a, first section, of the Tw (new) in conjunction with Article 1, heading and under i, of the Wbp[105], a legal ground is also required for the transfer and placement of data on the user's smartphone as enumerated in Article 8 of the Wbp.

WhatsApp has not stated and the investigation has not shown that WhatsApp bases the data processing activities conducted for this purpose on one of the legal grounds as specified in Article 8, heading and under b through f, of the Wbp.

With regard to the legal ground of unambiguous consent (Article 8, heading and under a, of the Wbp), the following applies.

The difference between 'consent' and 'unambiguous consent' is that in the latter case the controller must have no doubt whatsoever that the data subject has granted his consent.[106] In view of the overlap of these definitions, the consent requirement in Article 11.7a of the Tw (new) in conjunction with Article 1, heading and under i, of the Wbp corresponds in this respect with the legal ground of unambiguous consent (Article 8, heading and under a, of the Wbp). In light of the above, the circumstance that the (European) legislator found it necessary to require consent from the *user* for the transfer and placement of data means that if personal data is being processed (here, the mobile phone numbers of non-users in the address books on the smartphones of whatsapp users) in principle only the legal ground as stipulated in Article 8, heading and under a, of the Wbp, namely the unambiguous consent of the *data subject*, applies to this processing of personal data.

The data subject is the person about whom the data contains information (Article 1, preamble and under f, of the Wbp).

In practice, a data item can relate to more than one person at the same time. Each of those people is then the data subject for himself and the third party with respect to the others.[107] The mobile phone numbers of non-users contain (in any case) information about them. In view of this, they are data subjects for this processing of personal data. Users of whatsapp cannot grant (unambiguous) permission to WhatsApp, on behalf of the non-users in their address books, to process the contact data items related to them without being authorised to do so by the non-users in question. Only the relevant non-users themselves (or their legal representatives) can grant this consent.

---

[105] For this matter does not involve the technical storage of or access to data with the sole objective of enabling the information company to provide a service requested by the subscriber or user for which the storage of or access to data is strictly necessary (see also section 3.7 of this report). Cf. WP29 Advisory view 4/2012 on Cookie Consent Exemption of 7 June 2012. URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf.

[106] *Parliamentary documents II* 1997/98, 25 892, no. 3, p. 80.

[107] Idem, p. 63.

Because WhatsApp has not been granted unambiguous consent by non-users in the address books of whatsapp users to process their personal data and nevertheless processes that data, and WhatsApp also has no other legal ground for processing this data, WhatsApp is acting in breach of the provisions of Article 8 of the Wbp.

WhatsApp may first have to execute a number of processing activities related to the transfer procedure in order to assess whether the holders of the mobile phone numbers in the address books of whatsapp users have or have not granted their unambiguous consent for their data to be processed: or, to check whether WhatsApp has a legal ground for processing their personal data.

For that initial processing (short-term read access to the full address book of a whatsapp user), in addition to the requirement of unambiguous consent granted by the data subjects there can be a separate legal ground, provided that WhatsApp only uses this access to help the user identify which of his contact persons are already whatsapp users, and which therefore had already granted unambiguous consent in the past to WhatsApp to collect their mobile phone numbers and process them for this purpose. WhatsApp can possess a legal ground for this type of processing, a *compare and forget*, in Article 8, heading and under f, of the Wbp, WhatsApp's need to (be able to) comply with the provisions in the Wbp. In that case, the mobile phone numbers of non-users may only be collected and used for the strictly limited objective of verifying whether they have granted their unambiguous consent for their data to be processed, and they should be immediately deleted thereafter.

In its view (also in subsequent email correspondence), WhatsApp adopts the viewpoint that 'out-of-network' phone numbers (numbers of non-users of the app) are disidentified and hashed on the whatsapp servers in such a way that it is extremely difficult for WhatsApp (or third parties) to recover the original phone numbers. According to WhatsApp, in that respect it (already) involves a compare and forget system.[108]

In section 2.2 of this report, the Dutch DPA determined that the mobile phone numbers of non-users are not immediately deleted after verification that they have granted their unambiguous consent for the data to be processed. The out-of-network numbers are hashed and then stored and saved [CONFIDENTIAL: (...)].[109] In section 3.5 of this report, the Dutch DPA determined that there is (also) no question of disidentification by hashing, now that WhatsApp can recalculate the hashed out-of-network numbers and create a lookup table, for example, of all out-of-network numbers in readable (plain text) and hashed format. There is therefore no question of a compare and forget system. With respect to this point, therefore, WhatsApp's view has not led to a change in the conclusions in the report that WhatsApp has no legal ground for this data to be processed.

3.6.2 Status messages

[108] WhatsApp's view of 29 November 2012, p. 1.
[109] Declaration by WhatsApp during the conference call of 4 January 2013. See also OPC's email of 4 January 2013 to WhatsApp.

In section 2.5 of this report, the Dutch DPA determined that every whatsapp user can read the status messages of other whatsapp users, even the status messages of unknown users whose mobile phone numbers are in his address book.[110]

In section 3.5 of this report, the Dutch DPA determined that status messages, in combination with the mobile phone number and other customer and device identifiers, are personal data.

In response to the investigation conducted by the Dutch DPA and the OPC, WhatsApp has supplemented the information about status messages that it provides to its users.

The standard setting for status messages is: '*Hey there! I am using WhatsApp'*. A user can change this message in the app menu. If the user changes the message himself and enters his own text, in this specific case consent to process that information can in principle be deduced from his action.[111]

The OPC stresses in its preliminary findings that WhatsApp must build in extra safeguards against the risks of the widespread distribution of potentially sensitive information contained in status messages (for example, the user's exact location, or information about the user's health). Although, according to the Dutch DPA, on the basis of the available findings of the investigation there does not seem to be any formal breach of the Wbp, the Dutch DPA endorses the recommendation of the OPC that whatsapp users must be issued a warning, every time they change their status messages, that the message will be widely distributed (as a best practice). In its view, WhatsApp states that the addition of a warning/pop-up about the distribution of status messages − when users are adapting their status message – is now a priority on its product development agenda. With respect to this point, WhatsApp's view has not led to a change in the recommendation in the report.

3.7 Excessive use: access to the address books on smartphones

Elaboration of the legal framework

Article 11, first section, of the Wbp, stipulates, insofar as it is applicable to this investigation: *Personal data may only be processed insofar as, in view of the purposes for which it is collected or then processed, it is adequate, relevant and not excessive.*[112]

The objective for which the data is collected and then processed is a determining factor for the amount and type of data that is subjected to processing. In view of that objective, the data should not be excessive.[113]

---

[110] The Terms of Service and Privacy Notice state the following: '*Submissions may be globally viewed by users that have your mobile phone number, so don't submit or post status messages or profile photos that you don't want to be seen globally. A good rule of thumb is if you don't want the whole world to know something or see something, don't submit it as a Status Submission to the Service.'*

[111] Compare, amongst others, *Handleiding voor verwerkers van persoonsgegevens Wet bescherming persoonsgegevens* [*Manual for processors of personal data. Personal Data Protection Act*], Ministry of Justice, The Hague: 2002, p. 21-22. URL: http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/brochures/2006/07/13/handleiding-wet-bescherming-persoonsgegevens/handleiding-wet-bescherming-persoonsgegevens.pdf.

[112] This article is an implementation of Article 6, first section, under c, of the Privacy Directive.

Assessment
In its digital investigation into the app, the Dutch DPA ascertained that it was and is not possible for a user (except in the latest app version on an iPhone with version 6 of the iOS operating system) to complete the installation process without giving WhatsApp access to the mobile phone numbers of all other whatsapp users and non-users in his address book (see section 2.2 of this report).

In order for users to whatsapp with each other, it is not necessary for WhatsApp to collect all the mobile phone numbers from their address books and then use, record and store them. A user must have control over whether he wants to make the telephone numbers of his contacts available to WhatsApp, and if so, which contacts. He may only want to use whatsapp to communicate with one or two other users, and not with all the contacts in his address book.

In its view, WhatsApp points out that in the latest iOS version of the app (according to WhatsApp, the most commonly used operating system for the app), users have the option of refusing WhatsApp access to their electronic address books. If they have refused access in a dialog box displayed by the operating system, they can manually enter a phone number in order to send that person a whatsapp message.[114]

Because WhatsApp did not and does not give users the choice of using the app (except in the latest app version on an iPhone with version 6 of the iOS operating system) without granting WhatsApp access to the entire address book, or the choice of only allowing it to access selected contact persons with which they want to whatsapp (at that particular moment),[115] a large number of the mobile phone numbers collected from the address book was and is excessive. WhatsApp was and is therefore acting in breach of the provisions of Article 11, first section, of the Wbp. Because it is possible on the latest app version on an iPhone with version 6 of the iOS operating system to install the app and use it without granting access to the address book, with respect to these users WhatsApp is nog longer in breach of Article 11, first section, of the Wbp. In that respect, WhatsApp's view leads to adjustment of the conclusions in the report. For other operating systems, WhatsApp's view with respect to this point does not lead to any change in the conclusions in the report.

3.8 Retention period for the data of whatsapp users

Elaboration of the legal framework

Article 10, first section, of the Wbp stipulates that personal data may no longer be saved *in a format that makes it possible to identify the data subject, and only in a format necessary to realise the purposes for which it is collected or then processed.*[116]

---

[113] *Parliamentary documents II* 1997/98, 25 892, no. 3, p. 96.
[114] WhatsApp's view of 29 November 2012, p. 2.
[115] In view of the existing possibility for whatsapp users to invite their own new contacts and the possibility to install the app and use it without granting access to the address book in the latest app version on an iPhone with version 6 of the iOS operating system (see section 2.2 of this report), Whatsapp must also be deemed to be technically capable of programming a technical alternative.
[116] This article is an implementation of Article 6, first section, under e, of the Privacy Directive.

Sometimes the general time limit for which data can be stored is fixed in special legislation. Otherwise, the controller needs to ask himself whether there is a reason for continuing to store the data. If there is adequate reason, the controller can determine which time limits apply to the storage of that data. When those time limits have elapsed, the controller will no longer be able to process the data unless it is for a different but compatible objective.[117]

Assessment
In section 2.3 of this report, the Dutch DPA determined that WhatsApp saves the data of users for one year after they used their account for the last time. This can increase to a retention period of two years if the user installed the app and only tried it out once but did not actively cancel the account. The data relates to the mobile phone number, the account type and the cancellation date of the purchased service. In section 3.5 of this report, the Dutch DPA ascertained that this data is personal data. With regard to this personal data, no fixed minimum storage period has been defined in special legislation.

The current retention period for inactive users defined by WhatsApp itself means that on smartphones other than the iPhone data is or can be saved for up to two years if a user installs whatsapp free of charge (once-only), tries it out and then stops using it (for the iPhone, there is a subscription period of one year). There is no need for this long retention period in the case of inactive users. After all, once the free trial period or (paid) subscription period has expired, they can no longer use the app without (again) paying for it. Moreover, there are other, less radical ways of cleaning the data of inactive users. One widely-used method is to send one or more reminders to inactive users. WhatsApp has means of communicating with users. If a user does not react, his account can be cancelled automatically and the data erased.

WhatsApp states that it must have access to the data, particularly when it involves a paid account, during the *subscription* period in order to guarantee good service with no loss of quality (unless it involves data deleted by the user before the expiry date). [118] Above, the Dutch DPA determined, stating its reasons, that there is no need to store the data of inactive users for up to one year *after expiry* of the subscription period (and a maximum of up to two years on smartphones other than the iPhone). With respect to this point, WhatsApp's view therefore does not lead to a change in the conclusions in the report. In response to the investigation by the Dutch DPA and the OPC, WhatsApp has announced that retention periods and the information related to them are now a priority on its product development agenda, but it did not specify any dates.

In view of the above, the need for WhatsApp to save the data of inactive whatsapp users for as long as it now does has not been demonstrated.

WhatsApp is therefore acting in breach of the provisions of Article 10, first section, of the Wbp.

[117] *Parliamentary documents II* 1997/98, 25 892, no. 3, p. 95.
[118] WhatsApp's view of 29 November 2012, p. 2.

3.9 Security

Elaboration of the legal framework

Pursuant to Article 13 of the Wbp, the controller *should implement appropriate technical and organisational measures to protect personal data against loss or any form of unlawful processing. Taking into account the state of the technology and the costs of implementation, these measures must guarantee an appropriate security level in view of the risks related to the processing and the nature of the data to be protected.*[119]

The security obligation in this article extends to all components of the data processing procedure.[120]

The more sensitive the nature of the data, or the greater the threat to privacy due to the context in which the data is being used, the stricter the requirements to be defined for the security of the data. There is no obligation to always deploy the strictest security; the security must be adequate. Technical and organisational measures should be taken cumulatively (including, for example, security by means of passwords and encryption).[121]

'Unlawful forms of processing' include harming the data, unauthorised cognizance, modifying the data or supplying the data to others.[122]

Assessment

In section 2.4.1 of this report, the Dutch DPA ascertained that at the start of the investigation WhatsApp generated passwords using the WiFi MAC address on iPhones and the unique IMEI device number on other types of smartphones.

The use of the internal WiFi MAC address of smartphones involves major security risks. For a WiFi connection, a whatsapp user uses the WiFi MAC address of the smartphone. The smartphone is constantly broadcasting this MAC address in readable format, even if the connection is secure. In such cases, anybody within range of this WiFi network can use (free) network analysis software to intercept the MAC address and then pirate the password. [123]

It is easy to find out the MAC address even without using network analysis software. Anybody on the same WiFi network can look up the MAC address of every other device on that network in the lookup list for MAC addresses.[124]

There are also security risks associated with creating a password using the IMEI. Given the current state of the technology [CONFIDENTIAL: (...)], it is possible to create a lookup table of all possible IMEI numbers with the corresponding hash values. The computing power of graphical processors (GPU) will most likely increase exponentially in the future. At this point in

[119] This article is an implementation of Article 17, first section, of the Privacy Directive.
[120] *Parliamentary documents II* 1997/98, 25 892, no. 3, p. 98.
[121] Idem, p. 99.
[122] Idem, p. 98.
[123] [CONFIDENTIAL: (...)]
[124] The Address Resolution Protocol (ARP) uses lookup lists of MAC addresses of devices linked to the same network.

time, lookup tables with a length of twelve figures are freely available on the Internet. It is foreseeable that in the near future lookup tables of fifteen figures will also be available − that is, the length of the IMEI.[125]

In addition, [CONFIDENTIAL: (...)] advises against [CONFIDENTIAL: (...)] due to the risk of hash collisions – which means that different IMEI numbers can lead to the same hash value. One further risk with regard to the IMEI number is that other apps can also collect and process this number. [126] Processing often takes place in readable format, so that everybody within range of the WiFi network can intercept the IMEI number using freely available network analysis software. Another risk is that if an app developer with a large collection of IMEI numbers suffers a data leak, the IMEI numbers can become available on the Internet and others can therefore reproduce the password [CONFIDENTIAL: (...)].

The way WhatsApp created passwords and the ease, described above, with which they can be imitated exposed users to the real risk that others could pirate their passwords and then send and read messages using their accounts.

In section 3.5 of this report, the Dutch DPA ascertained that the messages, in combination with data about the sender and/or receiver, are personal data. And because whatsapp messages can contain sensitive, content-related information, WhatsApp's chosen working method resulted in unacceptable risks for the privacy of data subjects.

Because WhatsApp, in view of the sensitivity of the data, had not taken appropriate technical measures for the creation of passwords, WhatsApp was acting in breach of the provisions of Article 13 of the Wbp.

In response to the investigation by the Dutch DPA and the OPC, WhatsApp has adapted its working method in the sense that there are now app updates available that no longer use the WiFi MAC address or the IMEI device number, and instead use [CONFIDENTIAL: (...)], according to its view.[127] In section 2.4.1, the Dutch DPA determined that Whatsapp launched new updates of the app in December 2012 and forced active users to use the latest versions. Due to this combination of technical and organisational measures, following the update WhatsApp is no longer in breach of Article 13 of the Wbp with respect to active users. In that respect, WhatsApp's view leads to a change in the conclusions in the report.

There is still a risk with respect to the inactive users. The Dutch DPA has determined that inactive whatsapp users are not being confronted with a 'forced update'. WhatsApp has declared that finding a remedy for this risk for inactive users is now on its product development agenda, but it has not specified any dates.[128] With respect to that point, WhatsApp's view is (still) not leading to a change in the conclusions in the report. Because WhatsApp is currently not yet using the new method for all accounts, WhatsApp is still in breach of Article 13 of the Wbp.

---

[125] [CONFIDENTIAL: (...)]

[126] Wall Street Journal series 'What They Know Mobile'. URL: http://blogs.wsj.com/wtk-mobile/.

[127] WhatsApp's view of 29 November 2012, p. 2.

[128] Declaration by WhatsApp during the conference call on 4 January 2013.

In section 2.4.2 of this report, the Dutch DPA ascertained that at the start of the investigation by the Dutch DPA and the OPC, WhatsApp was using the app to send unencrypted messages. This meant that others were able to intercept the content of messages in readable format.

Due to the lack of any type of encryption of the data during transfer between the smartphone and the whatsapp servers − for example, SSL 'end-to-end' encryption, which is universally available and is an obvious security measure for the protection of this sensitive data − WhatsApp was acting in breach of the provisions of Article 13 of the Wbp.

In response to the investigation conducted by the Dutch DPA and the OPC, WhatsApp has taken measures to send the messages encrypted. WhatsApp is therefore no longer in breach of the provisions of Article 13 of the Wbp

4. CONCLUSIONS

WhatsApp, based in California in the United States, provides a service that is accessible to and expressly aimed at people in the Netherlands: the 'whatsapp' app. The app is now used by millions of Dutch smartphone users.

Because the app is being used to process personal data on smartphones in the Netherlands, the Dutch DPA is authorised to launch an investigation on the basis of the Dutch Data Protection Act (Wbp). This personal data includes the mobile phone number, unique customer and device identifiers and (where relevant) the push ID and the profile name of whatsapp users. In addition, WhatsApp processes the mobile phone numbers of non-users listed in the address books of whatsapp users. By its very nature, this data is related to the behaviour of natural persons (information on communication behaviour of people using the app). Moreover, WhatsApp can use the data – for example, the mobile phone number (which is a direct contact data item) − directly or indirectly, by means of intermediate steps, to track down an identifiable natural person (a whatsapp user or non-user).

WhatsApp uses the smartphones of whatsapp users − by way of the app that has been installed on the smartphones – as a means of processing personal data in the context of the app. The Wbp is imperative law, as is Chapter 11 of the Telecommunications Act (Tw). This means that its applicability cannot be excluded by a unilateral declaration or in the general provisions of a contract.

Access to the address book
People who want to use the app must grant WhatsApp access to their entire electronic address book, including the mobile phone numbers of contacts that are not using the app (except in the latest app version on an iPhone with iOS 6). Because WhatsApp does not obtain unambiguous consent from non-users to process their personal data and does not have any other legal ground for processing that data, WhatsApp is acting in breach of the provisions of Article 8 of the Wbp.

To enable users to whatsapp with each other, it is not necessary for WhatsApp to process all the mobile phone numbers in their address books. Because WhatsApp does not give users (except in the latest app version on an iPhone with iOS 6) the option of choosing whether they want to make their contacts available to WhatsApp and, if so, which contacts, a large number of the

mobile phone numbers collected from the address books are excessive. WhatsApp is therefore acting in breach of the provisions of Article 11, first section, of the Wbp.

Retention period
WhatsApp stores the personal data of inactive users for one year. Because WhatsApp has not demonstrated that the data of inactive users need to be stored for such a long time, WhatsApp is acting in breach of the provisions of Article 10, first section, of the Wbp.

Security
The way WhatsApp generated passwords – that is, using the hashed WiFi MAC address on iPhones and the hashed IMEI device number on other types of smartphones − exposed whatsapp users to the risk of others pirating their passwords and using their accounts to send and read messages. WhatsApp was therefore acting in breach of Article 13 of the Wbp. In response to the Preliminary Findings report, WhatsApp adopted a new method to create passwords. In December 2012, WhatsApp launched new versions of the app, and started to force active users to switch to these latest versions. Users are forced because they can no longer use the older versions of the app. There are still risks for inactive users that do not update their app. After all, users only obtain a new password when they *actively* install a new update. WhatsApp has stated that it will address these risks for inactive users, but it has not specified any dates. Because WhatsApp is currently not using the new method for all accounts, with regard to users whose passwords are still based on the WiFi MAC address or the IMEI device number WhatsApp is (still) acting in breach of the provisions of Article 13 of the Wbp.

When the Dutch DPA and the OPC started their investigation, Whatsapp was using the app to send messages unencrypted. This meant that others could intercept the message contents in readable format. In response to the investigation, WhatsApp now uses encryption. In this respect, WhatsApp is therefore no longer acting in breach of the provisions of Article 13 of the Wbp.

Status messages
Every whatsapp user can read the status messages of other whatsapp users, even those of unknown users, whose mobile phone numbers are listed in his address book. In response to the investigation conducted by the Dutch DPA and the OPC, WhatsApp has supplemented the information that it provides to its users about the distribution of status messages. The OPC stresses that WhatsApp must build in extra safeguards against the risks of the widespread distribution of potentially sensitive status information. Although in this respect there would seem to be no formal breach of the Wbp, the Dutch DPA endorses the recommendation of the OPC that whenever users of whatsapp change their status message, they should be warned that there is a risk of that message being widely distributed.

Announced measures
In response to the investigation by the Dutch DPA and the OPC, WhatsApp has announced that priorities on its product development agenda are: (i) addressing the residual risk in the password security of inactive users, (ii) retention periods and the information related to them and (iii) the addition of a warning/pop-up about the distribution of status messages, when users are adjusting their status message. WhatsApp has however not specified any dates.