Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
T. 0303 123 1113 F. 01625 524510
www.ico.org.uk

Anne Hoge
General Counsel
WhatsApp Inc.
By email only: hoge@whatsapp.com

Copied to Gareth Byrne, Associate General Counsel, WhatsApp Ireland Limited

16 February 2018

Dear Ms Hoge,

Sharing personal data between WhatsApp Inc. ("WhatsApp") and the Facebook family of companies

I write to inform you that I have concluded my investigation into the above.

I appreciate your engagement and constructive dialogue on this matter to date and your recent attendance at the Article 29 Working Party ("WP29") Taskforce meeting held on 25 January 2018, chaired by my office. The detail provided in this meeting and in your letter of 4 February 2018 has allowed me to understand WhatsApp's revised approach to the sharing of user data with Facebook Inc. and its other group companies ("Facebook").

As a result, I am minded not to exercise my powers to serve an enforcement notice under section 40 of the Data Protection Act 1998 (the "DPA") but instead to issue an undertaking setting out the terms we expect WhatsApp to agree to. This letter explains the purpose and scope of my investigation as well as my key findings.

Background

In 2014 WhatsApp was acquired by Facebook Inc. At that time the WhatsApp privacy policy did not provide for WhatsApp to share any personal data about users with Facebook. In fact, Facebook informed the European Commission that it would be unable to establish reliable automated matching between Facebook and WhatsApp user accounts[1].

On 25 August 2016 WhatsApp launched an updated version of its terms and conditions and its privacy policy. The new privacy policy indicated that WhatsApp would share users' personal data with "the Facebook family of companies" for three purposes:

(i) "The Business Analysis Purpose". This involves the use of personal data by WhatsApp and Facebook:

to help operate, provide, improve, understand, customize, support, and market our Services and their offerings. This includes helping to improve infrastructure and delivery systems.

[1] http://europa.eu/rapid/press-release_IP-17-1369_en.htm

(ii) "The System Security Purpose". This involves the use of personal data by WhatsApp and Facebook for:

fighting spam, abuse, or infringement activities.

(iii) "The Targeted Advertising Purpose". This involves the use of personal data by WhatsApp and Facebook:

to improve your experiences within their services such as making product suggestions (for example, of friends or connections, or of interesting content) and showing relevant offers and ads.

Existing users were notified of these changes when they launched the WhatsApp app. In relation to the sharing of personal data with Facebook for the Targeted Advertising Purpose, there was a facility for existing users to withhold consent to this, and also for them to withdraw consent during a period of 30 days after they signified agreement to the changes. There was no similar facility in relation to the sharing of personal data for the Business Analysis Purpose or the System Security Purpose.

Apart from the above, if a user did not wish to agree to the change to the terms and conditions and privacy policy they would need to stop using WhatsApp. New users would have to agree to the updated version of the terms and privacy policy in order to proceed with registration.

Purpose and scope of the investigation

The processing of personal data by WhatsApp and Facebook affects millions of UK citizens every day. The changes announced led to interest and scrutiny by the media, civil society groups and data protection authorities from across the world.

On 26 August 2016 I issued a statement advising that I would be looking into these changes and on 9 September 2016 I wrote to Facebook Ireland Limited, given the close relationship with WhatsApp, making initial enquiries and advising that I had launched an investigation into the matter.

My investigation set out to ensure WhatsApp is being transparent with users about how their personal data is being shared and to ensure users were able to exercise control over their personal data where relevant.

The original intention in matching account data may appear to be innocuous, and be driven by a desire to protect individuals. However, one of my concerns is privacy policy creep under the guise of normal updating activity. Once data has been matched it opens the door to further uses of the data which users might never have agreed to had they known, and may only require a minor change to the privacy policy which goes unnoticed. My role is to ensure that online companies are clear and accountable to their users about how they use and share personal data and provide appropriate ongoing controls.

Jurisdiction

Section 5(1)(b) of the DPA applies to data controllers using equipment in the UK for processing personal data. As WhatsApp processes personal data using equipment in the UK, through the smartphones of UK citizens who install and use WhatsApp, its processing of personal data of UK users comes within the DPA.

Summary of events

Since writing to Facebook Ireland Limited on 9 September 2016 advising that I had launched an investigation, my staff have regularly engaged with representatives of Facebook and WhatsApp directly and through the WP29. My letters of 23 September 2016 and 10 October 2016 set out my concerns about the processing in detail.

In a letter to my office dated 28 October 2016 Facebook Ireland Limited advised that the sharing of data had been 'paused' in relation to Facebook ads and product experiences. This indicated that WhatsApp was not sharing personal data with Facebook so that they could use such data for the Targeted Advertising Purpose for the benefit of their own businesses. This pause in the sharing of personal data from WhatsApp to Facebook did not cover "The Business Analysis Purpose" or the "System Security Purpose".

On 16 August 2017 WhatsApp published a new "Notice for EU users" among the "Frequently asked questions (FAQ)" on its website. This additional information for users provided some clarification about the nature and purpose of the sharing of personal data by WhatsApp with Facebook. However, it did not address all of the concerns highlighted in my letter, and was not actively communicated or given sufficient prominence to users. This means that despite welcome steps towards compliance during this time, our investigation has determined that there are key concerns still to be addressed.

Current position

On 25 January 2018 there was a meeting of representatives of WhatsApp and Facebook with the WP29 Taskforce. At this meeting, and in the subsequent written update, WhatsApp confirmed its current position on the sharing users' personal data with "the Facebook family of companies" for the three purposes;

1. WhatsApp advised that there was no current sharing of personal data for "the Business Analysis Purpose" on a controller-to-controller basis.

2. WhatsApp advised that there was no current sharing of personal data for "the System Security Purpose" on a controller-to-controller basis. However, you signalled your intention to commence sharing data for this purpose on a controller-to-controller basis further to user engagement planned later this year ahead of the General Data Protection Regulation (GDPR) coming fully into force.

3. WhatsApp confirmed the decision to indefinitely pause the sharing of personal data for "the Targeted Advertising Purpose". WhatsApp advised that there are currently no plans to unlock this form of personal data sharing.

Whilst WhatsApp does not currently share any data on a controller-to-controller basis, you indicated your intention to do so in relation to "the System Security Purpose" and that you may consider the 'legitimate interests' processing condition as your lawful basis of processing under Art 6(1)(f) of GDPR.

WhatsApp indicated that it works with Facebook as a service provider, meaning data is being shared on a controller-to-processor basis. This information cannot be used by Facebook for the benefit of their own businesses.

WhatsApp has stated that you do not collect personal data from users beyond that which is necessary to run your service. Data collected includes mobile telephone numbers, device information and which features are being used.

Key Findings

The first data protection principle states that:
"Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless—
(a) at least one of the conditions in Schedule 2 is met, and
(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met."

The second data protection principle states that:
"Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes."

After careful review of the information provided to me by WhatsApp and Facebook, I consider that WhatsApp would contravene the first and second data protection principles if you were to share users' personal data with Facebook so that Facebook could use such data for the benefit of its own businesses (i.e. on a data controller to data controller basis). This is the case whether the sharing is for the Business Analysis Purpose, the System Security Purpose, the Targeted Advertising Purpose or otherwise.

Your letter dated 28 October 2016 stated that the sharing of personal data with Facebook was only 'paused' for the Targeted Advertising Purpose. It is a fair assumption for me to make, that WhatsApp and Facebook may have been sharing personal data for the Business Analysis Purpose and the System Security Purpose on a controller to controller basis, but have at some point since that letter decided to pause sharing personal data for those purposes. This sharing, if it occurred, would have been in breach of the first and second data protection principles in the DPA.
Specifically I find that:

(i) WhatsApp has not identified a lawful basis of processing for any such sharing of personal data. Such sharing would contravene the first data protection principle.

(ii) WhatsApp has failed to provide adequate fair processing information to users in relation to any such sharing of personal data. For this reason also, such sharing would contravene the first data protection principle.

(iii) In relation to existing users, such sharing would involve the processing of personal data for a purpose that is incompatible with the purpose for which such data were obtained. This would contravene the second data protection principle.

I will now provide more detail as to why I consider reliance on consent and/or legitimate interests in order to provide a lawful basis for such sharing is insufficient based on the information provided to date.

Reliance on consent

One potential legal basis relied upon by WhatsApp for the sharing of data with Facebook is consent.

Consent is not defined in the DPA. However, the European Data Protection Directive (to which the DPA gives effect) defines an individual's consent as "*...any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.*" The fact that an individual must "signify" their agreement means that there must be some active communication between the parties.

WP29 published Opinion 15/2011 on the definition of consent, and set out that consent should be unambiguous, specific, informed and freely given. In particular, it specifies that consent must consist of a statement or clear affirmative action, be demonstrable, clearly distinguishable, intelligible and easily accessible, use clear language and be capable of being withdrawn.

My investigation has found that the process used and the information provided to users by WhatsApp has been seriously deficient as a means to inform their unambiguous and specific consent for each of the three purposes.

First, for the Business Analysis Purpose and the System Security Purpose, any purported consent from existing users and new users was too general (relating to the Terms and Conditions and Privacy Policy as a whole) rather than being specific to these particular uses. Neither existing users nor new users were given any opportunity specifically to give or withhold consent to the sharing of their personal data with Facebook for these purposes.

Secondly, any purported consent was neither genuine nor free. If a user did not wish their personal data to be shared with Facebook for the Business Analysis Purpose or System Security Purpose, the only option was to cease using WhatsApp (in the case of existing users) or not to begin using it (in the case of new users). This is also true for new users in relation to the Targeted Advertising Purpose.

Thirdly, any purported consent was not fairly obtained. In relation to existing users, the process did not inform users with sufficient clarity that their personal data was to be shared with Facebook for any of the purposes. The first layer of the notice did not mention Facebook at all, and a significant percentage of users will not have read any further. The Key Updates summary was more likely to confuse users, as it was likely to be read by many as a positive indication that personal data is not shared with Facebook.

In relation to new users, there is nothing in the course of the sign up process that specifically alerts them that, by agreeing to the Privacy Policy and the Terms and Conditions, they are agreeing to share their personal data with Facebook. Still less is there anything that specifically alerts them that they are agreeing to do so for the specific purposes.

Fourthly, any purported consent that was not obtained on a properly informed basis. WhatsApp did not provide an explanation (other than in very general terms) of what was involved in the any of the purposes. In particular, WhatsApp did not provide a clear explanation of how users' personal data will be used by Facebook for the benefit of the Facebook group companies (rather than of WhatsApp). Nor has WhatsApp provided a clear explanation as to what personal data of users will be shared with Facebook.

Moving forward, the new General Data Protection Regulation ("GDPR") sets a higher standard for consent. The GDPR is clearer that an indication of consent must be unambiguous and involve a clear affirmative action by the user, with consent only being an appropriate lawful basis if a user is offered control and genuine choice.

Reliance on legitimate interests

Schedule 2 paragraph 6 of the DPA recognises that controllers may have legitimate reasons for processing personal data that the other conditions for processing do not specifically deal with. The "legitimate interests" condition is intended to permit such processing, provided you meet certain requirements.

There are three elements to the "legitimate interests" condition:
- identify a legitimate interest;
- show that the processing is necessary to achieve it; and
- balance it against the individual's interests, rights and freedoms.

A key factor in this balancing exercise is whether or not users have been given a clear explanation of the scope of processing which is to be undertaken. Users should understand how their personal data is to be used and therefore be able to make an informed decision whether or not to continue to use a service such as WhatsApp. Without this, the balance will tend away from the controller's legitimate interests, unless there is a real risk of harm to other individuals.

My investigation has found that WhatsApp's privacy policy and terms and conditions currently lacks a sufficiently clear explanation regarding the scope of any potential processing to enable WhatsApp to rely on the legitimate interests condition, in all but

exceptional circumstances, such as a real risk of serious harm to an individual. Although in that situation, another Schedule 2 condition is likely to apply.

I recognise that there will be a range of legitimate interests WhatsApp could demonstrate. This may include sharing personal data for purposes such as fighting spam and business analytics. In each case I expect WhatsApp to be able to work through and demonstrate the three elements listed above, considering safeguards such as data minimisation and pseudonymisation. I expect Data Protection Impact Assessments to be conducted before data is shared for any purpose. For the System Security Purpose, I expect a DPIA to be conducted at a general level, to inform urgent and specific decisions which may need to be made at a later date.

During our conversations you indicated that WhatsApp wants to rely on legitimate interests to share information about 'bad actors' identified on your platform. Both WhatsApp and Facebook emphasised your commitment to the safety and security of your users and combatting abuse.

Where WhatsApp is able to identify a specific legitimate interest, show that the processing is necessary to achieve it, and balance it against the individual's interests, rights and freedoms, then you may be able to share information (providing you meet the other conditions set out in the undertaking). I expect you to be able to demonstrate your reasoning to me if requested, including why the sharing was necessary and proportionate to ensure the safety and security of the users of your platform.

I want to emphasise that clearly there will be situations where such sharing is appropriate. For example, if you have identified instances of online child abuse or similarly serious activity, and sharing personal data with Facebook might detect or prevent this activity from continuing on another platform.

The Undertaking

WhatsApp has, since this investigation begun, responded to feedback regarding user control and transparency. I recognise that WhatsApp is known as an innovative firm and market leader whose business relies upon the trust of its users. In addition to the importance of compliance with data protection laws there is a genuine opportunity here to show users that WhatsApp are a business that is responsive to UK user concerns, providing transparency, choice and control to UK citizens.

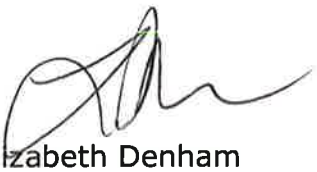
In order to bring your data processing into compliance with the DPA I propose that WhatsApp agree to the terms set out in the enclosed undertaking by 2 March 2018.

On its return, the undertaking will be signed by myself and the text will be published on the ICO website. A copy of the signed document will then be returned to you for your records. You should note that any significant breach of a signed undertaking will likely lead to enforcement action being taken by my office.

Publicity

My office aims to be an effective, open and transparent regulator. Given that this case affects millions of UK users it is likely to attract wide public and specialist interest. I therefore intend to take a proactive approach to sharing the details of our investigation. I plan to publish this letter on 6 March 2018 regardless of whether or not you sign this undertaking. I hope that you and we continue to work co-operatively to ensure your users experience the highest standard of data protection.

Yours sincerely,



Elizabeth Denham
Information Commissioner