Office of the Privacy Commissioner of Canada | Commissariat à la protection de la vie privée du Canada

6100-010588

FINAL REPORT OF FINDINGS

Investigation into the personal information handling practices of WhatsApp Inc.

January 15, 2013

REPORT OF FINDINGS

Our File: 6100-010588

Complaints under the *Personal Information Protection and Electronic Documents Act* (the "Act")

1. On January 26, 2012, the Office of the Privacy Commissioner of Canada initiated a complaint against WhatsApp Inc. ("WhatsApp"), a California corporation, pursuant to subsection 11(2) of the Act, having reasonable grounds to believe that it was collecting, using, disclosing and retaining personal information in a manner contrary to certain provisions of Schedule 1 of the Act.

2. The investigation was conducted in collaboration with the Dutch Data Protection Authority (College bescherming persoonsgegevens) and focused on alleged privacy violations concerning consent, limiting collection, limiting use and retention, and safeguards. The investigation was limited to privacy issues identified during the period January 26, 2012 through November 30, 2012.

3. WhatsApp was notified of the complaint on February 16, 2012 and cooperated fully with our investigation.

4. Representations were received from WhatsApp from March 22, 2012 through to January 4, 2013. On October 15, 2012, based on the results of our investigation, our Office issued a preliminary report of investigation to WhatsApp ("Preliminary Report"). In our Preliminary Report, we made recommendations to WhatsApp with the aim of ensuring that it was meeting its obligations under the Act vis-à-vis the issues we investigated. This report of findings reflects those recommendations and WhatsApp's response.

Introduction

5. WhatsApp Inc. owns and operates “WhatsApp Messenger” (hereafter “the application”), a cross-platform mobile messaging service which allows individuals to exchange messages on their mobile devices through the Internet rather than by short message service (SMS). The application is available on a variety of mobile devices and platforms, including Apple’s iPhone, Research in Motion’s BlackBerry, and Google’s Android. In addition to basic messaging, the application allows users to send and receive images, video and audio media messages.

6. WhatsApp is a US corporation registered and headquartered in California. WhatsApp actively promotes and distributes its service to Canadians. At the time our investigation was initiated, the application was considered one of the top-five best selling apps in the world, and was widely used by Canadians. By some estimates, the application is said to facilitate the transmission of over one billion messages per day globally.

7. At the time our investigation was initiated, a subscription to use the application cost $0.99. The application operates free of advertising, and messages sent and received using the application are free of charge to users, but for applicable network data fees. According to WhatsApp, it does not currently sell marketing data and does not share personal information with third parties. Personal information means information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization.

Enrolment and account registration

Issue

8. Based on a technical review of the application, our Office initiated a complaint in respect of WhatsApp’s service registration process to investigate whether that process allowed for unauthorized access to a user’s account, contrary to Principle 4.7 of Schedule 1 of the Act. More specifically, this Office investigated whether a user’s WhatsApp account could be used prior to the completion of the user authentication process, thereby

allowing a third party to create and control accounts associated with phone numbers which they did not own.

Summary of Investigation

9. Individuals may download WhatsApp's messenger service from a variety of on-line stores. In some cases, the application is pre-loaded to an individual's phone by a network carrier or device manufacturer.

10. Once the application has been downloaded to a mobile device, an individual is required to register with WhatsApp using his or her mobile device.

11. During the registration process, individuals are asked to read and accept WhatsApp's Terms of Service and Privacy Policy. The Terms of Service and Privacy Policy are provided in a pop-up window at the time of registration and are also available on-line on WhatsApp's website.

12. Once an individual has read and accepted WhatsApp's terms of service, he or she is asked to specify the country in which they reside and to provide their mobile phone number. In some cases, the application may also ask a registrant for their preferred notification name (i.e., the name the user wishes to appear in out-going messages).

13. According to WhatsApp, once an individual has provided his or her country code and mobile telephone number, the application collects the following information from the registrant's mobile device: device identifier information, mobile subscriber ID, mobile country code, and mobile network code.

14. Using that information, WhatsApp sends an account confirmation message to the registrant by way of standard SMS. Using the registrant's reply to that message, WhatsApp then verifies that the personal information provided by the user during the registration process matches that attached to the mobile device. Once confirmed, a user is registered and his or her account is activated. The user may then begin sending and receiving messages with other WhatsApp users world-wide.

15. Notwithstanding the verification procedures above, in early 2011 it was reported in various technical reviews that WhatsApp's registration process allowed for the application's use even in cases where a user failed to respond to WhatsApp's account confirmation message. In other words, even in cases where a registrant failed to authenticate, the application would verify the registered device and allow for the transmission of messages to that device.

16. It was further reported that WhatsApp's account confirmation messages were being sent using ordinary web traffic ports, allegedly without encryption or safeguards. Absent appropriate security measures, confirmation messages and any personal information attached thereto ran the risk of being intercepted. Once intercepted, a confirmation number could be used to access and receive a user's messages and/or any other personal information sent to the programmed number (as detailed in the paragraphs following).

Application of the Act

17. In making our determination on this issue, we applied Principles 4.7 and 4.7.1 of Schedule 1 of the Act. Principle 4.7 requires that personal information be protected by security safeguards appropriate to the sensitivity of the information. Principle 4.7.1 goes on to say that an organization's security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use or modification.

18. In our view, a registrant's device identifier information, mobile subscriber ID, mobile country code, and mobile network code constitute personal information under the Act, since that information, alone or in combination with other information, could render a specific individual identifiable.

19. According to WhatsApp, it first identified the registration issues outlined above in May 2011. Upon becoming aware of the potential for a security breach in registration, and prior to the initiation of our investigation, WhatsApp took measures to correct the problem.

20. In order to assess the accuracy of publicly reported registration flaws, and to confirm that the remedial actions undertaken by WhatsApp were sufficient in ensuring compliance with the Act, customized tests were performed of WhatsApp's registration process. Based on the test results, we were satisfied that issues identified with respect to WhatsApp's mobile registration process had been resolved.

Finding

21. Based on the results of our testing, and following confirmation from WhatsApp that it is not aware of any security issues outstanding relating to its registration process, we find concerns relating to the matter of WhatsApp's registration process to be **not well founded.**

Integration with a user's address book

Issue

22. Based on a technical review of the application, our Office initiated a complaint to investigate whether WhatsApp was collecting more personal information than necessary for the purposes of allowing its users to send and receive messages, contrary to Principle 4.4 of Schedule 1 of the Act. We also investigated whether WhatsApp required the upload of a user's *full* address book or contact list as a condition of service – as opposed to allowing for the use of contact information belonging only to those individuals a user chose to communicate with – contrary to Principle 4.3.3 of Schedule 1 of the Act.

Summary of Investigation

23. WhatsApp's messenger service provides an instant messaging system that can be used across mobile devices, whether BlackBerrys, iPhones, Windows-based phones or Androids. BlackBerry users, for example, may message Android users and iPhone users, and vice versa – a feature generally not available on the proprietary messaging systems built into phones by mobile manufacturers. In order to send and receive

messages using the application, however, both the sender and recipient of a message must have the application installed and registered on his or her device.

24. In order to facilitate contact between application users, WhatsApp relies on a user's address book to populate his or her WhatsApp "All Contacts" list. Once a user consents to the use of his or her address book, contact information from the user's mobile device is periodically transmitted to WhatsApp's servers to assist in the identification of other WhatsApp users.

25. According to WhatsApp, the application is designed to upload a user's mobile address book to WhatsApp's servers up to two times daily, or as initiated by the user during a contact refresh. According to WhatsApp, personal information collected during the contact discovery process is limited to mobile numbers. WhatsApp contends that it does not collect the names, email addresses or other information stored in a user's address book. Association between contact names and numbers occurs on a user's device only, and not by virtue of any data matching by WhatsApp.

26. Once a user has consented to the use of his or her contact information for contact discovery, mobile numbers from the user's address book are transferred securely to WhatsApp's servers using Secure Socket Layer / Transport Layer Security or SSL/TLS encryption.

27. Once uploaded, a contact number is categorized by WhatsApp's corporate servers as being either "in-network" (i.e., registered with WhatsApp) or "out-of-network". Only numbers listed as in-network can be contacted using the WhatsApp service. An out-of-network number would only become associated with a WhatsApp user once the application was installed and registered on a device with that number.

28. According to WhatsApp, in-network numbers are stored as original values (i.e., in clear text) on their servers. Out-of-network numbers are stored as one-way, irreversibly hashed values. WhatsApp uses a multi-step treatment of the numbers, with the key step being an "MD5" hash function. The phone number and a fixed salt value serve as input to the hash function, and the output is truncated to 53 bits and combined with the

country code for the number. The result is a 64-bit value which is stored in data tables on WhatsApp's servers. According to WhatsApp, this procedure is designed to render out-of-network numbers (i.e., the mobile numbers of non-users) anonymous.

Application of the Act

29. In making our determination on this issue, we applied Principles 4.3.3 and 4.4.1 of Schedule 1 of the Act, and subsection 5(3) of the Act. Principle 4.4.1 precludes organizations from collecting personal information indiscriminately. By law, the collection of personal information must be limited to that which is necessary for stated purposes identified by an organization.

30. Principle 4.3.3 states that an organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use or disclosure of information beyond that required to fulfill the explicitly specified and legitimate purposes.

31. Subsection 5(3) of the Act states that an organization may only collect, use, or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

32. At the time our investigation was initiated, paragraph 3B of WhatsApp's Terms of Service provided the following information to users on the collection and integration of contact information:

> *In order to access and use the features of the Service, you acknowledge and agree that you will have to provide WhatsApp with your mobile phone number. You expressly acknowledge and agree that in order to provide the Service, WhatsApp may periodically access your contact list and/or address book on your mobile device to find and keep track of mobile phone numbers of other users of the Service...*
>
> *You hereby give your express consent to WhatsApp to access your contact list and/or address book for mobile phone numbers in order to provide and use the Service. We do not collect names, addresses or email addresses, just mobile phone numbers.*

33. According to WhatsApp, if a user withholds consent for the upload or integration of address book information, the application may continue to operate, but in a limited or degraded manner only. Users are not able to send and receive messages to individuals of their choice through the manual input of single or proposed contacts.

34. In the course of our investigation, customized tests were performed of the application's contact discovery process. Based on the test results, we confirmed that personal information collected during the contact discovery process is limited to mobile numbers only.

Recommendations and Finding

35. Principle 4.4 of Schedule 1 of the Act provides that the collection of personal information must be limited to that which is necessary for the purposes identified by the organization. Principle 4.5.3 states that personal information that is no longer required to fulfil the identified purposes should be destroyed, erased or made anonymous.

36. Notwithstanding the fact that information collected by WhatsApp during its contact discovery process is limited, users should have the ability to manually add and manage contacts, rather than being compelled to provide their complete address books in the identification of other application users. At the time our investigation was initiated, WhatsApp required users to consent to the collection and use of all the phone numbers in their address books as a condition of service, rather than allowing a subscriber to use the individual phone number of the contact he or she wishes to correspond with.

37. Furthermore, since WhatsApp does not require the mobile numbers of non-users in order for the application to function, we recommended in our Preliminary Report that those numbers be destroyed immediately after their identification and classification as "out-of-network" numbers. While non-user numbers may be collected with a user's consent in the course of the application's contact discovery process, those numbers should not be retained by WhatsApp.

38. WhatsApp has instead implemented a procedure to render out-of-network numbers "anonymous". Although our preference was to see those number deleted, according to

WhatsApp, the collection and retention of both in-network and out-of-network numbers is necessary to facilitate the operation of its application.

39. In order to render out-of-network numbers anonymous, WhatsApp employs a cryptographic hashing technique which, in its view, renders the original value of out-of-network numbers difficult to determine. According to WhatsApp, this hashing process precludes the identification of non-users, providing subscribers of the service on the one hand with an effective mechanism to find new contacts, while on the other hand protecting the mobile numbers of non-users.

40. In the course of our investigation, we reviewed technical flowcharts and functional narratives supporting WhatsApp's anonymization process for out-of-network numbers. We also spoke with a member of WhatsApp's engineering team in an effort to better understand the underlying logic supporting the company's anonymization process.

41. Based on our review of the above process, we found that WhatsApp's treatment of out-of-network numbers was not an effective form of anonymization. True anonymity is only achieved where information can *never* be linked to an individual, either directly or indirectly**.** In our view, WhatsApp's use of all digits in an out-of-network phone number, coupled with a fixed salt value for the hash function, does not result in a true anonymization of out-of-network numbers. This is because the number could be recovered, with a modest amount of computing effort, if the out-of-network number database and salt value were breached. Indeed, simple test programs created by our technical experts showed that phone numbers could be recovered, once the salt is known, in under 3 minutes using a standard, low-power desktop computer. The fact that the phone numbers can be recovered – albeit through a data breach and some computing effort –means that the storage is not truly anonymous.

42. Furthermore, we note that re-submitting the same telephone number to the process will always result in the same value, so the company could adopt a practice (or be compelled) to reprocess a phone number and find it in their databases.

43. Although WhatsApp has stated that their treatment procedure will result in some overlap in attempts to recover out-of-network numbers (i.e., "intentional collisions"), making it possible that multiple numbers produce the same hashed results (and thus offering

some privacy protection to non-users), the small amount of overlapping values does not, in our view, provide a sufficiently practical form of anonymity.

44. Although personal information collected by WhatsApp during the contact discovery process is appropriately limited to that necessary for legitimate purposes, as specified by WhatsApp in its Terms of Service, the company's retention of out-of-network numbers remains, in our view, unnecessary and may create the potential for inappropriate or unintended uses of non-user mobile numbers.

45. Based on the above, and whereas out-of-network numbers are being retained for longer than required for purposes of contact discover, we find concerns relating to the retention of non-user numbers to be **well founded**.

46. Notwithstanding the above, further to recommendations in our Preliminary Report, WhatsApp now provides iPhone users with the option to manually add contacts, thus by-passing the application's contact discovery process. Our tests confirm that such functionality has now been built into its latest Apple iOS application (version 2.8.7). According to WhatsApp, the same functionality is to be integrated into its implementation plan for other operating systems, though the company could not provide us with a firm commitment date for that implementation.

Automatic sharing of status messages

Issue

47. Based on a technical review of the application, our Office initiated a complaint to investigate whether WhatsApp was failing to obtain the knowledge and consent of individuals prior to disclosing their personal information, contrary to Principle 4.3 of Schedule 1 of the Act. More specifically, we investigated whether WhatsApp was broadcasting the "status updates" of its users to individuals the user may not know (or may not wish to share personal information with), without their knowledge and consent.

Summary of Investigation

48. WhatsApp allows its users to populate and share “user status submissions” (e.g., brief expressions of a user’s state of mind, his or her location, and or opinion). In order to enter his or her status, a user must open the application’s “Status” tab where he or she may input a personalized message or select one of several default status settings. Standard messages include “available”, “busy”, “at school”, “at work”, “sleeping”, “in a meeting”, and “urgent calls only”.

49. Personalized status submissions are limited to 139 characters. While a user’s status field cannot be left blank (except for users of Apple’s iPhone), it can be populated with random characters, punctuation or graphic illustrations (i.e., so called “emoticons”) so as to render the status message meaningless. Once the user has input his or her status submission, he or she is prompted to “save” the status or cancel its entry.

50. Once saved, a user’s status submission is ready for broadcast. Except for the legal terms attached to user status submissions, as provided for in WhatsApp Terms of Service and Privacy Policy, no further prompts or instructions are provided to users prior to the broadcast of a status message.

51. In contrast to some social networking platforms which allow an individual to limit or control the broadcast of status submissions to only certain people, status messages shared using the WhatsApp messenger service are, by design, broadcast to all WhatsApp users who have the broadcasting user’s telephone number in their contact list. As such, a sender may not have knowledge of the identity of all those application users who may be receiving or monitoring the sender’s status messages. Any individual, whether for friendly or nefarious purposes, may track a user’s status, so long as that individual has the message sender’s telephone number.

52. At the time that our investigation was initiated, WhatsApp provided users with a lengthy explanation of the terms of use associated with user status submissions. WhatsApp disclosed the non-confidential nature of status submissions to all users in its Terms of Use and Privacy Policy, as follows:

The WhatsApp Service permits the submission of status text and other communications submitted by you and other users.

You understand that whether or not such User Status Submissions are published, WhatsApp does not guarantee any confidentiality with respect to any submissions.

You shall be solely responsible for your own User Status Submissions and the consequences of posting or publishing them.

Any status content that you submit to the WhatsApp Sites may be redistributed through the internet and other media channels, and may be viewed by the general public.

53. According to WhatsApp, status updates are refreshed periodically over the course of a day. Where a user manually refreshes his or her contact list, the status update for that specific user's in-network list will also be updated.

54. Status messages are not shared with individuals who are blocked by the sender (i.e., individuals added to the user's "blocked contacts" list).

55. In addition to user defined status updates, WhatsApp may also provide "last seen" activity notifications to those listed in a subscriber's in-network. "Last seen" activity reflects the approximate time at which a user last used the application or otherwise brought the application to the foreground. Unlike the broadcast of user status submissions, the distribution or publication of last seen activity can be limited through a user's profile settings.

Application of the Act

56. In making our determination on this issue, we applied Principles 4.3, 4.3.2, 4.3.4 and 4.3.5 of Schedule 1 of the Act. Under Principle 4.3, the knowledge and consent of an individual are required for the collection, use or disclosure of personal information, except where inappropriate. Under Principle 4.3.2, in order make consent meaningful, the purposes for which personal information is to be used must be stated in such a

manner that an individual can reasonably understand how the information will be used or disclosed.

57. Principle 4.3.4 speaks to the form of consent an organization must seek prior to the collection, use or disclosure of personal information. Recognizing that forms of consent may vary, Principle 4.3.4 requires that an organization take into account the sensitivity of the personal information in question. Principle 4.3.5 states that the reasonable expectations of the individual are also relevant in obtaining consent. Although some information is almost always considered sensitive, any information can be sensitive depending on the context.

58. In investigating the matter, we first considered whether or not a user's status submission constitutes "personal information" under the Act. As previously stated, subsection 2(1) of the Act defines personal information as information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization.

59. Consistent with relevant jurisprudence, our Office is of the view that information will be about an "identifiable individual" where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other information. Even subjective information about an individual may still be personal information, whether or not that information is held to be accurate.

60. We note further that information is still personal information even where it is publicly available within the meaning of the Act's regulations (though such information may be exempt from applicable consent requirements).

61. In keeping with the interpretation of personal information above, we believe that information contained in a user's status submission may constitute personal information. There are innumerable instances where a user may elect to share information about him or her self – whether location, opinion, the status of a relationship, or some other self-expression – and where such information, alone or in combination with other data, would render the individual identifiable.

62. Accepting that a user's status submission may constitute personal information, the Act requires that WhatsApp ensure and obtain the knowledge and consent of an individual prior to the collection, use or disclosure of that information. Consent must be meaningful and, whether implied or express, must bear in mind the potential sensitivity of the personal information in question and the reasonable expectations of the individual involved.

63. In the complaint at hand, our primary concern rests with the inability of the user to limit and control the broadcast of his or her status messages. While we accept that a user who chooses to supply personal information in his or her status submission is electing to share or broadcast that information with others, the unlimited or unknown dissemination of that information is not in our view within the reasonable expectations of the application user.

64. Bearing in mind the nature of the application – a peer to peer messaging platform, where users may only communicate with those listed in their private address books – we find it hard to believe that a user would consent to the sharing or broadcast of personal information beyond his or her contacts, and/or to application users unknown to him or her. While the application allows for the suppression of status broadcasts to individuals listed in a user's "blocked contact" list, that list can only be populated with individuals who the user knows.

65. Unlike some micro-blogging services, whose primary function is to enable both users and non-users to read or receive text-based messages through a range of services and platforms, WhatsApp's mobile messaging system (as described by WhatsApp itself) is first and foremost an SMS replacement. It allows for the instant communication of messages to targeted or specific individuals, as identified by the application user. While the application may also provide a user with the ability to more widely share personal expressions or status messages, it does so under the umbrella of peer to peer communications, conveying the general impression that such messages are being shared only with those people the user knows.

66. As explained in paragraph 51, WhatsApp does not allow for granular control over the distribution of status submissions. While the application is functionally capable of blocking users from receiving status messages (including "online" and "last seen"

information), the effective use of the blocking feature requires a user to list or identify that person who he or she wishes to block. Doing so may not be possible however where the unwanted user is unknown to the message sender.

67. Given the above, and where status messages are likely to be seen as being shared only with specific and known recipients, we would have expected WhatsApp to have provided better notice of the potentially indiscriminate nature of status broadcasts.

68. Notwithstanding WhatsApp's efforts to describe status submissions as non-confidential, in our view, information pertaining to the application's status functionality was not (at the time our investigation was initiated) sufficiently clear and visible to users. Where the application's design precludes a user from limiting or controlling the dissemination of status messages, WhatsApp has a duty to ensure that users of status submissions are informed in the simplest and clearest terms that what they say on WhatsApp may be viewed by any and all WhatsApp users around the world instantly.

69. During the course of our investigation, WhatsApp amended its Terms of Service and Privacy Policy to better inform users of the public nature of broadcast messages. As of September 2012, the Policy disclosed, in part, the following:

> *Status Submissions…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…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 of 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 to be seen globally.*
>
> *A good rule of thumb is <u>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</u>…You understand*

that whether or not such Status Submissions are published, WhatsApp does not guarantee any confidentiality with respect to any submissions. [our emphasis]

Recommendation and Finding

70. As previously noted, Principle 4.3.2 requires knowledge and consent for the collection, use and disclosure of personal information. Notwithstanding recent efforts to update WhatsApp's Terms of Service and Privacy Policy, in our view, further efforts are required to advise users of the potentially widespread or indiscriminate broadcast of personal information through status submissions.

71. Whereas WhatsApp's Terms of Service and Privacy Policy may not be readily available to users on mobile devices, and whereas WhatsApp is not yet able to avail its users with more granular control over the broadcast of status messages, in our Preliminary Report we recommended that WhatsApp provide real-time notification for broadcast messages. It is our view that real-time or active notification would allow for more meaningful consent for the broadcast of status submissions. We appreciate of course that, to avoid a disruption of application enjoyment, users should be given control over notification prompts and default settings.

72. In response to our recommendation, WhatsApp has stated that it has added real-time notification (e.g., pop-ups) for user status submissions to its future implementation plan. According to WhatsApp, real-time notification is to be integrated into future application releases beginning September 30, 2013.

73. Where WhatsApp has committed to advising users of the widespread dissemination of personal information through status submissions in its Terms of Service and Privacy Policy and by way of real-time pop-ups, we find the complaint on the matter of the automatic sharing of status messages to be **well founded and conditionally resolved**.

Offline storage of messages

Issue

74. Based on a technical review of the application, our Office initiated a complaint to investigate whether WhatsApp was contravening the retention provisions of the Act. More specifically, we investigated whether WhatsApp did not have appropriate guidelines in place to govern the retention of undelivered messages, contrary to Principle 4.5.3 of Schedule 1 of the Act.

Summary of Investigation

75. Messages sent using the WhatsApp service are first transmitted to corporate servers co-located at secured facilities in Washington DC and Virginia using a subscriber's regular data service. Where the intended recipient is online, those messages are routed by WhatsApp to their designated addressee.

76. Delivered messages are not retained by WhatsApp. According to WhatsApp, the company does not maintain a record or archive of messages delivered. Records of delivered messages are saved only on the user's mobile device and may be deleted or retained by the user at will.

77. In cases where the intended recipient of a message is found to be off-line, messages sent to that recipient by other WhatsApp users are stored by WhatsApp, pending delivery. An undelivered message may be saved by WhatsApp for up to 30 days, after which the message is automatically deleted.

78. Messages not delivered are mapped to one of four server partitions. Within each partition, one file is reserved for each user. According to WhatsApp, silo 'ing is controlled on a per user basis by nature of the operating system file. In its representations to our Office, WhatsApp confirmed that it limits its retention of undelivered messages to 30 days.

79. At the time our investigation was initiated, WhatsApp did not provide users with information relating to its retention policy for personal information, whether in its Terms of Service, Privacy Policy or Licensed Application End User License Agreement.

Application of the Act

80. In making our determination on this issue, we applied Principles 4.5.2, 4.5.3 and 4.8 of Schedule 1 of the Act. Principle 4.5.2 provides in part that organizations should develop guidelines and implement procedures with respect to the retention of personal information. These guidelines should include minimum and maximum retention periods. Principle 4.5.3 states in part that an organization shall develop guidelines and implement procedures with respect to the destruction of personal information. Under Principle 4.8, an organization is obliged to make specific information about its policies and practices relating to the management of personal information readily available.

81. Where messages may be archived or maintained by a user on his or her mobile device following delivery, and where communications between users are intended primarily for instant messaging, we find WhatsApp's retention period of 30 days for undelivered messages to be satisfactory in the circumstances.

82. Notwithstanding the above, we would have expected WhatsApp to have described its general retention policy for personal information in its Terms of Service, Privacy Policy or Licensed Application End User License Agreement. As required under Principle 4.8, individuals should be able to acquire information about an organization's policies and practices without reasonable effort. As well, given that message delivery is central to WhatsApp's management of personal information, and in light of Principle 4.5.2, WhatsApp ought to have developed, implemented and communicated procedures for the retention and destruction of personal information contained therein.

Recommendations and Finding

83. In light of the above, we recommended in our Preliminary Report that WhatsApp develop guidelines and ensure the implementation of procedures with respect to the retention of

personal information. We further recommended that WhatsApp make readily available to users information relating to WhatsApp's retention policy surrounding the off-line storage of messages.

84. In response to our recommendations, WhatsApp has committed to further develop its retention policy for personal information and to make the revised policy publicly available. WhatsApp has agreed to update and expand its Terms of Service and Privacy Policy by March 31, 2013 so as to provide better notification of those policies to its users.

85. Based on the above, we find the complaint on the matter of message retention to be **well founded and conditionally resolved**.

Transmission security

Issue

86. Based on a technical analysis of the application, our Office initiated a complaint to investigate whether WhatsApp was adequately protecting personal information, in contravention of Principle 4.7 of Schedule 1 of the Act. More specifically, it was alleged that messages sent and received using the WhatsApp service were not being encrypted, rendering personal information contained in such messages subject to eavesdropping or interception.

Summary of Investigation

87. As previously stated, WhatsApp's messaging system is intended to replace standard SMS. The application uses a mobile user's data service (rather than telephone service) to send and receive instant messages.

88. At the time that our investigation was initiated, messages sent using the application were not encrypted. As such, messages sent and received using the application ran the risk

of interception, especially where a user elected to use the service through unprotected Wi-Fi networks.

89. In the course of our investigation we confirmed that messages sent between application users were not secure. Even in cases where data was sent over ports used for secure https (SSL/TLS) communications, personal data including the content of user messages and telephone numbers were clearly visible.

Application of the Act

90. In making our determination on this issue, we applied Principle 4.7 of Schedule 1 of the Act. Principle 4.7 requires that personal information be protected by security safeguards appropriate to the sensitivity of the information. Principle 4.7.1 provides that security safeguards must protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use or modification.

91. Recognizing that the contents of messages sent between application users may at times be sensitive personal information, we would have expected WhatsApp to have employed sufficient safeguards to ensure the security of those messages.

92. In its representations to our Office, WhatsApp confirmed that messages sent and received using the application were not being encrypted – affirming the need to introduce safeguards to ensure the security of instant messages and any other personal information attached to those messages.

93. In partial response to our concerns, in September 2012 WhatsApp began adding protocol encryption to its mobile messaging service. If properly applied, the end-to-end encryption would appropriately safeguard messages from eavesdropping or interception.

94. As at the time our investigation concluded, WhatsApp had implemented encryption for several devices, including Nokia's S40, Research in Motion's BlackBerry, Apple's iPhone, and all Windows and Android based phones.

Recommendation and Finding

95. Notwithstanding changes made by WhatsApp to encrypt user messages, in the course of our investigation we noted that WhatsApp was using the MAC addresses of iPhone devices to auto generate passwords for message exchanges with the WhatsApp service. On other mobile smart phones, the IMEI number of the phone was being used instead. MAC and IMEI numbers are identifiers that are unique to each phone and which are typically assigned by device manufacturers.

96. In light of the risks associated with the exposure of IMEI numbers and MAC addresses, and where methods of generating passwords using IMEI and MAC addresses are relatively well known, the use of the IMEI or MAC for the purpose of generating a password on behalf of the user does not, in our view, provide sufficient security for personal information exchanged using the WhatsApp service. According to our technical experts, this practice created a serious risk that a user's password could be replicated without authorization and that messages might be intercepted by a third party without the user's knowledge or consent.

97. Based on the above, in our Preliminary Report we recommended that WhatsApp develop new protocols for the creation of encryption passwords for iPhone devices. In response to our recommendation, WhatsApp has stopped using IMEI and MAC numbers for authentication on all mobile platforms. WhatsApp has stated that the application is now using a 160-bit randomly generated key.

98. In order to confirm the implementation of the newly developed password process, we reviewed technical flowcharts and functional narratives supporting WhatsApp's authentication process. We also reviewed and studied real examples of that process with the assistance of technical experts. Our goal was to understand how the underlying logic supporting authentication worked so as to assess whether or not the process, as designed by WhatsApp, was sufficiently safeguarding personal information.

99. Based on the results of our investigation, and as at the time that our investigative work ended, the security safeguards employed by WhatsApp appeared to be commensurate

with the sensitivity of personal information at risk. As such, we find the complaint on the matter of transmission security to be **well founded and resolved**. We nonetheless encourage WhatsApp to remain vigilant when protecting personal information in light of a constantly changing threat environment.

Data retention and account termination

Issue

100. Based on a technical review of the application, our Office initiated a complaint to investigate whether WhatsApp was retaining the personal information of its users following account deactivation, contrary to Principle 4.5 of Schedule 1 of the Act. More specifically, we investigated whether WhatsApp continued to retain the personal information of its users even where the application had been uninstalled.

Summary of Investigation

101. At the time our investigation was initiated, both technical and user reviews of the application alleged that WhatsApp was retaining the personal information of subscribers subsequent to the removal of the messenger service from their mobile devices.

102. According to these reviews, in order to have their personal information deleted, users were required to notify WhatsApp of their request by email. These procedures, often onerous, were not publicly available, whether in WhatsApp's frequently asked questions document, or in WhatsApp's Terms of Service and Privacy Policy.

Application of the Act

103. In making our determination on this issue, we applied Principles 4.5.2, 4.5.3 and 4.8 of Schedule 1 of the Act. Principle 4.5.2 states in part that an organization should develop guidelines and implement procedures with respect to the retention of personal

information. These guidelines should include minimum and maximum retention periods. Principle 4.5.3 states in part that an organization shall develop guidelines and implement procedures with respect to the destruction of personal information. Under Principle 4.8, an organization must make specific information about its policies and practices relating to the management of personal information readily available.

104. As previously discussed, messages delivered using the WhatsApp service are not retained by WhatsApp. Only undelivered message are saved by WhatsApp, and then only for 30 days pending delivery, after which time such messages are automatically deleted.

105. Further to the above, it is WhatsApp's policy to delete or destroy all personal information belonging to a user, including any applicable payment information, 30 days after termination of the service. According to WhatsApp, the retention of billing information, if any, for 30 days after termination is to provide users with a short period of time for ease of renewals or registration. After the 30-day period post account expiry, a user may sign up again for WhatsApp's service, but will have to go through the registration process anew.

106. An exception to WhatsApp's 30-day retention period exists where an individual uses the application for a one year free trial period and fails to subscribe as a paying user. Where a trial user elects not to renew his or her subscription following one year of service, select personal information of that individual (including the trial user's name, telephone number, and account type) may be retained for up to one year. According to WhatsApp, this information is retained so as to ensure that a trial user cannot re-subscribe for a successive free trial period.

107. While we find WhatsApp's retention guidelines for personal information to be satisfactory on the whole, once again we would have expected WhatsApp to have described its retention policy for personal information in its Privacy Policy or other readily accessible documentation.

108. As required under Principle 4.8, individuals should be able to acquire information about an organization's policies and practices without reasonable effort. Where data retention is central to WhatsApp's management of personal information, WhatsApp ought to have

developed, implemented and communicated procedures for the retention and destruction of personal information.

Recommendations and Finding

109. Based on the above, in our Preliminary Report we recommended that WhatsApp develop guidelines and ensure the implementation of procedures with respect to the retention and destruction of personal information. We further recommended that WhatsApp make readily available to users information relating to WhatsApp's retention policy for personal data.

110. As previously stated, in response to our recommendations, WhatsApp has committed to further developing its retention policy for personal information and to making this policy publically available. WhatsApp has agreed to update and expand its Terms of Service and Privacy Policy by March 31, 2013 so as to provide better notification of those policies to its users.

111. Based on the above, we find the complaint on the matter of user data retention to be **well founded and conditionally resolved**.