

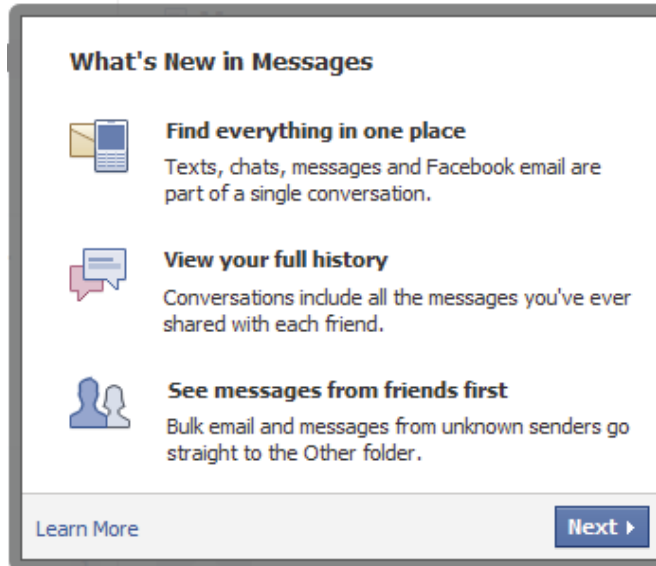
Facebook Content as Digital Evidence

Implications of Facebook's Updated Messages Feature




For any questions on this report, or to learn more about Cernam's work around online evidence and investigations, please get in touch via email, see www.cernam.com or contact us via Twitter, [@CernamOE](https://twitter.com/CernamOE).

Owen O'Connor
(@CernamOwen)
owen@cernam.com
+353 1 716 3793

Karen Reilly
(@CernamKaren)
karen@cernam.com
+353 1 716 3784



What's New in Messages

-  **Find everything in one place**
Texts, chats, messages and Facebook email are part of a single conversation.
-  **View your full history**
Conversations include all the messages you've ever shared with each friend.
-  **See messages from friends first**
Bulk email and messages from unknown senders go straight to the Other folder.

[Learn More](#) [Next ▶](#)

Background: Facebook Content as Digital Evidence

From its origin as a site for college students to share photographs Facebook has developed into one of the most popular and sophisticated messaging systems in the world, with close to 700 million users exchanging 4 billion messages each day. Facebook interactions increasingly document the life of its users, making Facebook content a rich source of potential evidence in criminal investigations, lawsuits, employment disputes and other contexts.

Collecting and preserving online evidence is our core focus at Cernam and the popularity of Facebook makes it one of the most high-profile sources of online evidence. This paper summarizes recent research we have undertaken around a significant Facebook change currently being rolled out: the upgraded Messages system. The new Messages system, fundamentally changes the nature of Facebook and the associated risks, for example providing users with a web-based mail system and adding support for Office documents and other attachments.

We believe that New Messages will have a profound impact on digital evidence and in particular on electronic discovery in civil litigation, comparable to the launch of Google's Gmail in 2004. Our goal is to begin highlighting the implications of Facebook New Messages now, while the system is still being rolled out, so that professionals dealing with online evidence will be better prepared when they first encounter New Messages.

Introducing New Messages, the updated Facebook messaging system

In November 2010 Facebook announced an overhaul of their Messages feature and the release of what they called “a modern messaging system”. At that time Facebook Messages allowed simple text communication between users on an asynchronous basis, i.e., where users could interact without both being online at the same time. The Messages system did not allow attachments but was otherwise similar to email: messages could be sent to one or more Facebook users and consisted of a subject line and message body, similar to an email.

Facebook's New Messages feature generated significant media attention in late 2010 with references to “Project Titan” (Facebook's internal codename) as “the Gmail killer” and “the future of email”. At the announcement of New Messages last November Mark Zuckerberg stated “This is not an email killer. This is a messaging experience that includes email as one part of it”. Zuckerberg went on to say that New Messages “fundamentally alters the way people communicate”, a claim which is difficult to dispute having looked at the scope of New Messages.

While launching New Messages, Facebook detailed the usage of their previous system, stating that 350 million people were actively using Messages and that those users generated 4 billion messages each day. To put this level of usage in perspective, the top three webmail providers (Gmail, Yahoo! and Hotmail) have around 800 million users between them. Facebook's new system therefore changes the way that 350 million people communicate, making it

very clear that New Messages will be important as a source of digital evidence.

Why Now?

Facebook's rollout of New Messages began last November but initially affected relatively few users. Based on the relevance of New Messages to online evidence Cernam has followed New Messages closely and in May we noticed that many users in Ireland, the UK and other locations outside of the US were being switched to New Messages. Although the new system is still not fully available this recent expansion brings in many more users and may signal more aggressive deployment. It also represents our first chance to try out the new system directly, since several of our team have switched to New Messages. We have therefore begun analyzing aspects of the new system relevant to digital evidence, leading to a series of articles on our website and to this paper.

Key Features of Facebook's New Message

“Next Generation Messaging”

Facebook define the key attributes of “a modern messaging system” as seamless, informal, immediate, personal, simple, minimal and short. New Messages has been built around these concepts and incorporates SMS messages, email and chat to interweave all communication across all of a user’s devices. With this seamless communications experience Facebook aims to make New Messages the central place where users integrate and control all of their private communication, both within Facebook and externally.

Users of Gmail will recognize another key feature of New Messages: the use of conversations or threads to group related messages visually. Unlike Gmail however, Facebook’s interface uses threads to store a complete history of all communication with a given person. A distinct thread is created for each Facebook contact, meaning threads are not based on a time period or a particular topic, and all types of communication are included: Facebook Messages, Facebook Chat, SMS text messages and email.

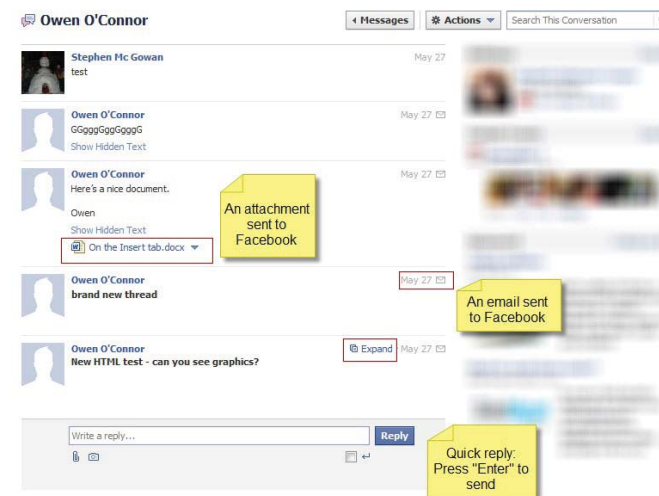
For many Facebook users the conversion to New Messages has been jarring since familiar elements have been removed and the new system functions more like an instant messaging system, to the extent that some users have labeled it “Chatmail”. For example, when composing a message users cannot set a subject line and there are no options for familiar email options such as “cc” or “bcc” (this happens to be the easiest way to tell whether your account has been upgraded – if your messages have subject lines you do not have New Messages!). Sending a message is as simple as hitting the enter key with no further decisions required, a simplification which Facebook has highlighted as a key benefit since it reduces the number of tasks required to send a message digital evidence.

The Social Inbox

Not unlike Gmail’s “Priority Inbox”, Facebook’s New Messages ranks the importance of each conversation. Messages from Facebook friends or “friends of friends” appear in the main inbox folder, while messages from other users will initially be diverted to a separate folder labeled “Other”. The default message view also highlights messages from friends so that these will always appear first in the message listing.

Since Facebook Messages now supports email the system must also filter and prioritize external messages. By default new messages received via email from non-Facebook users will be routed to the “Other” folder. If a user consciously moves a conversation to the Inbox this decision will be respected for all future messages, meaning new emails from that sender will appear in the inbox.

Facebook users can also opt to block messages from non-friends so that these will not appear in either their inbox or “Other” folder. Finally messages can be archived which hides them from the main messages view, similar to LinkedIn’s messaging system. If a new message is received in an archived conversation the entire conversation will be moved back to the active inbox. At this point it appears that message threads cannot be deleted from the archive and instead can only be moved back to the main inbox.



Facebook Email

Perhaps the largest and most obvious change in the rollout of New Messages is the introduction of Facebook.com email addresses for users of the new system. Users are not required to use a Facebook email address in order to use Messages but must create one in order to receive messages from non-Facebook users. The new email address is based on the Facebook username, e.g., username “johndoe123” would produce an email address of “johndoe123@facebook.com”. If a user has not yet selected a username they will be required to do so when switching to New Messages.

Facebook users and non-users alike can use a Facebook.com email address to send messages via their normal email system, for example from a corporate mail system or a webmail provider such as Gmail or Hotmail. When a Facebook user sends an email from Facebook Messages to an external email address the email is formatted as a Facebook message and includes a profile picture and a link to the relevant Facebook profile.

Send and Receive Messages from your Phone

If a user chooses to incorporate text messaging into their Facebook Messages the text messages they share with Facebook friends will be integrated into the relevant New Messages conversations along with all other interactions. This also means that a user who is offline can send a message to a Facebook friend by texting the short code

“32665”. For example, texting “msg John Doe Hello” will send the message “Hello” to a Facebook friend named John Doe, and that text message will then appear in the Messages conversation between the two users. In addition if John Doe is not logged on to Facebook at the time the message may be relayed as a text message or email.

Unified Messaging

Facebook designed the new Messages system so that there is a sense of continuous conversation. The user can choose which services they want to avail of: chat, email, SMS. If the user is online, they will receive messages in real time through Facebook chat whether the sender had communicated via email, chat or SMS. If the user is not online, Facebook will choose the most appropriate option for sending the message to the user. If a user goes offline mid-conversation, the other user can continue writing their message and it will be sent as a text or email. In this way Facebook has removed the need for users to select either a synchronous messaging option (Facebook Chat) or an asynchronous one (old-style Facebook Messages).

Top 5 things you need to know

This recent upgrade fundamentally changes the nature of Facebook Messages and therefore breaks many widely-held assumptions about the limitations and use of Facebook as a messaging platform. In this section we will therefore highlight 5 of the most important features for anyone interested in Facebook Messages as evidence, for example in litigation or employment matters.

#1: Facebook is now a webmail system

Our first key point regarding “New Messages” is that interactions are no longer limited to Facebook users. In fact the new features effectively make Facebook a webmail system, comparable to Gmail, Hotmail or Yahoo! Mail.

As we noted previously, the 3 largest webmail providers (Gmail, Yahoo! and Hotmail) have around 800 million users – 800 million combined, with the largest (Hotmail) having around 360 million users. Comparing this to Facebook’s almost 700 million users makes it easy to see the potential impact of New Messages, particularly given that the current Messages system has 350 million active users. If a majority of these existing users adopt the Facebook.com email system, Facebook will quickly become one of the world’s largest webmail providers.

If New Messages proves popular it could lead certain users to shift their traditional email interactions away from their current email system. More importantly Facebook has stated that they will provide access to messages via the “IMAP” protocol which would allow users to configure iPhones and other mobile devices to use Facebook email addresses. Users could also access their Facebook messages from email programs such as Outlook and Apple Mail, or from within other webmail systems such as Gmail. In this scenario it is very likely that some users would shift to Facebook.com email and potentially stop using or even close their accounts on other services.

Widespread use of Facebook email will lead to the same issues seen with personal webmail accounts in general: employees forwarding

business records to personal addresses; interactions with colleagues shifting away from corporate systems; business correspondence being sent via personal accounts; use of personal accounts rather than remote access when travelling, etc. In essence corporate email systems are already in competition with services such as Gmail or Hotmail and for many users the simplified minimal nature of Facebook Messages may be compelling, particularly given strong support for mobile devices.

In addition to business data we can be confident that government records will also make their way into Facebook messages, since the use of personal webmail accounts has already been highlighted by high-profile cases such as those of Senator John Ensign and Governor Sarah Palin. Similar cases exist in other jurisdictions but have not reached similar prominence, for example in Ireland a cabinet minister used a personal email for government business while out of the country.

#2: Facebook now supports attachments

One major advance brought by New Messages is that users can now send Office documents and other attachments through Facebook. Files can be attached to messages within Facebook or to emails being sent externally via Facebook.com email addresses. Although most mobile apps for Facebook have yet to be updated for the new system it is also likely that mobile attachment sending will be possible as apps are upgraded.

Unlike other webmail providers Facebook has not detailed their mailbox or attachment size limits, instead pointing to a comment from Mark Zuckerberg who said “if you are a good user and don’t try to test the limits, you should be fine”. This unwillingness to copy the “we give you more storage” positioning of other webmail providers is a further key difference in Facebook’s approach to messaging: it is clear that they view their strengths as ease of use and integration with Facebook, not the ability to store gigabytes of data.

Since Microsoft Office files represent the bulk of corporate documents it is important to note that Facebook offer specific features for working with Office files. In the past this has been done through Microsoft’s “Docs.com” online service, however New Messages uses “Office.com”. This is also a Microsoft service but one which is entirely separate to Docs.com, meaning files which were previously viewed, created or edited using Docs.com will not be visible through New Messages. This integration allows Facebook users to receive an Office document view New Messages and view or edit it directly in their browser, without requiring a copy of Office.

The ability to exchange attachments greatly increases the risk that business documents will be stored within Facebook accounts, particularly with the strong features around Office documents which may lead employees to upload or email files in order to view them on a mobile device or a system without Office.

#3: Facebook conversations are now logged by default

Prior to New Messages Facebook did not offer logging for conversations via Facebook Chat, unlike other instant messaging systems where users can choose to enable or disable logs. New Messages now integrates email, Facebook messages, Facebook chat and cellphone text messages into one social inbox with a complete record of all interactions with each contact. As a result Facebook is now logging chat contents by default so that they can be stored and displayed alongside other interactions, with no ability to disable logging or temporarily enable an “off the record” mode. This greatly expands the universe of potential Facebook evidence and brings in a far more informal channel which could prove valuable in litigation.

Another interesting aspect of chat logging is the ability to add new people to an existing conversation, even if that conversation was started by another person. After adding a new participant that person can view all of the previous messages in the conversation. This feature could be a straightforward way to provide attorneys or investigators with access to past content, however it is also likely that it will be used for bullying and harassment.

Finally on this issue, we have seen instances of Facebook chat conversations appearing in the New Messages system where the chat conversation occurred many months ago, prior to the introduction of New Messages. This suggests that although Facebook did not expose chat logs at that time, chat logs were being created and are now being exposed via the new interface.

#4: Facebook’s “Data Download” tool is dangerously incomplete

In October 2010 Facebook began rolling out a new feature which allowed users to download their Facebook information. This “data download tool” is advertised as providing an export of all information shared via Facebook, with the data being downloaded in the form of a zip file. The download includes photo albums, details of events, wall content, profile information, friend lists and messages.

Several e-discovery and digital evidence experts have recommended that this data download tool could be used to gather evidence from Facebook and have even suggested that this is one of the intended purposes of the tool. Based on our research, which will be published shortly at www.cernam.com, we have significant concerns about the use of this tool for any evidential purpose and particularly for gathering evidence in e-discovery.

Having looked again at the data download tool in the context of New Messages we feel confident in stating that the data downloaded is dangerously incomplete and inaccurate, making it entirely unsuitable for any evidential purpose. In essence it appears that Facebook have not updated the download to work with the new messaging system, for example the new system now integrates 4 types of communication in a single inbox, yet the data download shows only the traditional or old-style Facebook Messages. Facebook emails, text messages and logged chat conversations are entirely omitted, giving a highly inaccurate and misleading view of a conversation.

#5: That “Delete” button may not do what you expect

A final key point relates to an issue which we have not yet directly reproduced but which has been widely reported by users of New Messages: the reappearance of previously deleted messages. Certain users who have been switched to New Messages are re-discovering messages which they had previously deleted and which were not visible in the legacy Messages inbox. These messages appeared to have been entirely deleted, however the switch to New Messages has “resurrected” them and they are now visible in the unified inbox of New Messages.

The implication of this is that Facebook had implemented a “hide” feature rather than a true delete function but again this is not something we have been able to reproduce directly in our testing. For digital evidence professionals, attorneys or others with an interest in Facebook content as evidence, this “un-delete” issue represents a significant opportunity. It may be possible for example to prove that a user deleted certain messages, potentially destroying evidence or selectively pruning their inbox to support a particular position.

New Messages, New Difficulties

The introduction of New Messages radically changes Facebook's communications features and introduces several changes which may cause difficulties in digital investigations or e-discovery.

A radically different view of email

As we have noted, users who switch to New Messages will receive a Facebook.com email address based on their choice of username, for example the username "JDoe" would give an address of "JDoe@Facebook.com". New Messages will generate emails when a user communicates with another Facebook user who is offline or when an email address is entered as the recipient of a Facebook message. Facebook users can also receive external emails via their Facebook.com address, with emails being delivered to the Messages inbox.

At a basic level this description might seem similar to Gmail, Hotmail or other web-based email systems in that users compose and receive messages via their browser. However, New Messages represents a radically different view of email which will present issues for current e-discovery processes and technology. For example, a typical email has one or more recipients in the "To" header and may have optional "cc" and "bcc" headers indicating additional recipients. A Facebook.com email uses a distinctly different format and has no concept of "cc" or "bcc", instead using a single recipient line which can mix email addresses and Facebook usernames.

The second key omission you will notice when looking at a Facebook.com email is the lack of a subject line. An email generated by a person-to-person Facebook conversation will have a subject similar to "Conversation with John Smith" while a group conversation will be labeled "Conversation with John Smith and others", highlighting the person who started the thread. However, individual messages do not have a subject line and when composing

a new Facebook message there is no option to specify a subject. When an external email is received the original subject line is moved into the body of the message, meaning the original message is altered to some degree. These differences may make it difficult to group or de-duplicate Facebook.com messages for review and will also have the effect of removing key contextual information.

Collecting evidence from new Messages

For some digital evidence professionals Facebook New Messages will be a boon, providing a new source of data which documents informal interactions in a highly (albeit unusually) structured format. In particular the fact that Facebook users can exchange documents and other attachments via New Messages will be beneficial in many cases. Unfortunately exploiting this evidence will first require an appropriate method of collecting New Messages data as evidence.

We will address separately the many issues we have found with Facebook's "Download your Data" tool, a feature which many have suggested is tailor-made for evidence collection. For now it is sufficient to note that the data download tool was significantly flawed before the launch of New Messages, with key items of data omitted or incorrectly recorded in the exported zip file. After testing the data download tool on Facebook accounts which have been switched to New Messages our concerns have increased: in essence the exported data is dangerously incomplete and renders the tool completely unsuitable for evidence collection.

To give just one example of the issues with Facebook's data download function, if a user has switched to New Messages and has exchanged messages using the new system their exported data will omit all Facebook chat messages. More worryingly, if two users have exchanged Facebook messages and then one of the users sends an email to the other users Facebook email or adds an email address to the conversation, the entire conversation will be omitted from the data export. As such, the new system is effectively a remote control for causing messages to be omitted from the export tool. Consider a scenario where two colleagues have corresponded using old-style Facebook messages in a conversation which subsequently becomes relevant to litigation or a disciplinary matter. Either party to the conversation could prevent the other from exporting the contentious messages by responding to the previous thread using an email address.

In addition to these issues with the official Facebook data download tool there is currently no facility to download messages via IMAP, POP3 or other common email interfaces. Although these interfaces are far from ideal for collecting email from web-based mail systems they would offer at least a stop-gap method for collecting Facebook messages for electronic discovery. Facebook have stated that IMAP support is under consideration but at this time there is no easy method to preserve or collect data within New Messages.

New Messages, old assumption

New Messages fundamentally changes the way users interact on Facebook. For digital evidence or legal professionals who have previously worked with Facebook evidence this means setting aside old assumptions and starting afresh. Many professionals are

unaware for example that Facebook users can now exchange attachments, a change which significantly changes the risk model around Facebook Messages. As noted previously, the email element of New Messages also differs significantly from more traditional webmail systems which may lead to difficulties.

In investigating Internet email many investigators rely on the ability to view the internal email headers which represent the path taken by a message between various email servers, details of the email systems involved, important timestamps associated with a message, etc. In the New Messages investigators will find it difficult or impossible to view the headers for emails received using Facebook: at present there appears to be no method to view headers. Experienced investigators will also be disappointed, though perhaps not surprised, to find that Facebook do not include details of the sending computer in the headers of email sent using New Messages. This feature of traditional webmail systems such as Hotmail and Yahoo! Mail greatly simplifies email investigations; however it is understandable that Facebook would omit this feature given the current interest in online privacy.

Finally one key assumption which must now be reset is that an organization which blocks Facebook has removed the risk associated with Facebook messages in the workplace. Despite blocking access to Facebook as a website organizations will now find that staff are interacting with Facebook friends and engaging in group conversations via email using Facebook.com email addresses. The enhancements to Facebook's email experience make it possible to engage far more fully via email and will increase the need to address Facebook content as evidence in litigation or disciplinary matters.

Facebook New Messages & Digital Evidence: Looking on the Bright Side

Although we have mainly discussed negative aspects of New Messages, for example the risks introduced by the webmail feature, there are aspects of the system which will be helpful in using Facebook Messages as evidence.

Facebook Chat conversations are now logged

As noted previously, Facebook Chat conversations are now logged. Logging is a key feature in many instant messaging systems and the presence, absence or ability to control logging has an impact on how users interact. For example, most Skype users are aware that Skype instant messages are logged by default, potentially making Skype more or less suitable for different types of conversation. In the past Facebook did not log Chat messages by default and in fact provided no logging feature even for users who preferred to store conversations. Facebook users therefore have an expectation that Chat content is temporary and not stored.

With the introduction of the integrated inbox an interaction via Facebook Chat is just another Messages interaction and will be added to the conversation thread for the relevant user. For example, if John Smith and Jane Doe use Facebook email on Monday and Facebook Chat on Wednesday, their inboxes will show a single conversation containing both types of content. This will cause confusion for both users and digital evidence professionals in the short term, not least in terminology where we need to distinguish “New Messages” (the platform) from “Messages” (the asynchronous interaction which is just one type of New Messages interaction).

Overall however this change will be beneficial to investigators since confusion and broken assumptions among Facebook users will inevitably lead to sensitive conversations being logged without the participants’ awareness, particularly given that New Messages is

being rolled out gradually. It is easy to imagine, for example, office colleagues using Facebook Chat to discuss work issues specifically because they believe it is not logged. Once any participant in the conversations switches to New Messages the Chat conversations will be stored in their inbox and could be obtained in the context of electronic discovery or an internal investigation.

Switching to New Messages can resurrect old content

Although Facebook’s updated Messages system represents a significant improvement it has not been universally popular. Searching for comments on Twitter, Facebook or blogs will show a large number of Facebook users experiencing problems with New Messages, for example receiving incorrect notifications of message arrival.

By far the most interesting complaints deal with content unexpectedly appearing in the integrated inbox of New Messages. In particular there are many reports of previously deleted messages re-appearing following the switch to New Messages. This re-appearance of deleted messages has caused significant confusion since the users had specifically removed those messages and believed they had been erased.

Other users switching to New Messages have discovered that Facebook Chat sessions which occurred months before their upgrade are now in their integrated inbox. In other words, Facebook enabled Chat logging some time prior to deploying New Messages without informing users or providing a way to access the logs. To

date our direct assessment of New Messages at Cernam has involved just a handful of Facebook accounts, however we have already seen this issue which suggests it may affect a majority of users. These two issues – “zombie” messages and premature Chat logging – present a great opportunity in terms of Facebook data as digital evidence. The resurrection of previously-deleted messages can undo attempts to conceal or destroy evidence and in an extreme case could prove attempted spoliation. Similarly the fact that users believed Chat messages were not logged could lead to more candid discussions or more sensitive details being shared in Chat sessions, the contents of which could be made available by a switch to New Messages.

Authenticating Facebook.com Email Messages

We have discussed previously the fact that Facebook New Messages introduces a Facebook.com webmail system. As Dr Nathaniel Borenstein of Mimecast has noted, Internet email is far more complex than it first seems and Facebook may have a steep learning curve ahead. However, Facebook is off to a good start in one regard: their use of an email standard called “DKIM”.

DKIM stands for DomainKeys Identified Mail and is an Internet standard for digitally signing elements of Internet emails. DKIM aims to fight spam by allowing mail servers verify the source of email as it is received. For example, if a Google server receives a message which purports to have come from Yahoo! Mail it can quickly verify the signature and discard any messages which originate elsewhere, i.e., those which have fake email headers.

In addition to Google and Yahoo! many large email services implement DKIM, however its use is far from universal and it is good news that Facebook has adopted the standard. The implication from a digital evidence viewpoint is that emails generated by New Messages will be difficult to fake, or at least easy to prove as fake.

We will come back to the mechanics of authenticating emails using DKIM in a future article on our website since we believe this is a technique which is significantly under-used in digital forensics. For now the key point to understand is that Facebook’s implementation of DKIM means it will be possible in many cases to prove whether a given email truly came from Facebook and potentially even whether a specific account was used.

Other Investigative Benefits

The changes introduced by New Messages are so wide-ranging that it may be months before all of the details are fully understood. For example, New Messages introduces an additional method to find a Facebook user by email address: if a user with New Messages sends an email to an external email address that address will be changed to a Facebook profile ID in the conversation view. From our limited testing this function appears to work even if a user has opted not to have their profile searchable by email address.

Since the differences in New Messages, such as Facebook.com email and attachment support, make it a valuable source of digital evidence it may be useful to determine which users have the new system. Since users on the legacy Messages and new system cannot be mixed on a group message it is possible to determine who does

and does not have New Messages by simply composing a message.

The above method is useful provided an investigator has access to New Messages but other methods also exist. For example, the use of Facebook usernames as the left-hand side of New Messages email addresses makes it possible to determine externally whether an account has been upgraded: “username@facebook.com” will be a valid email address if the account has New Messages. Lastly an investigator with access to corporate web proxy logs or other network data can search for references to “fbstx.com” (a domain name used for HTML emails received via New Messages) which may identify internal users who are actively using New Messages.

Finally we would like to highlight the unusual nature of group conversations on New Messages. For example, adding a new participant to an existing conversation gives that person access to all previous messages, a potentially useful feature in dealing with harassment or with co-operating employees in e-discovery. When encountering group discussions in email we suggest looking closely at the “Reply-To:” header which directs responses to the group rather than to individuals. These addresses include the ID number (“FBID”) of the person who started the conversation and can be used to obtain full names and other profile details using the Graph API.