



# FIELD ANALYSIS REPORT

Regional Analysis with National Perspective.



29 September 2015

## (U//FOUO) Going Dark – Covert Messaging Applications and Law Enforcement Implications

(U//FOUO) Prepared by the Wisconsin Statewide Information Center (WSIC) with a contribution from the DHS Office of Intelligence and Analysis (I&A).

(U//FOUO) **Scope:** This Field Analysis Report explains covert messaging technology and its increasing use by both malicious actors and mainstream consumers. We are providing this analysis to inform local, state, and federal entities of potential adversary communication techniques that impact law enforcement and national security interests.

### (U) Summary

- (U//FOUO) Consumer demand has led to the rapid proliferation of covert messaging software applications, or apps.
- (U//FOUO) Covert messaging software can encompass off-network messaging and/or secure (encrypted) messaging.
- (U) Law enforcement access to data communicated over these platforms is increasingly problematic.
- (U//LES) Foreign terrorist organizations, homegrown violent extremists (HVEs), domestic terrorist and criminal organizations are integrating this technology into their operations.<sup>\*,†</sup>
- (U//LES) Understanding covert messaging apps is crucial for law enforcement investigators.

<sup>\*</sup> (U//FOUO) DHS defines an HVE as a person of any citizenship who has lived and/or operated primarily in the United States or its territories who advocates, is engaged in, or is preparing to engage in ideologically motivated terrorist activities (including providing support to terrorism) in the furtherance of political or social objectives promoted by a foreign terrorist organization, but is acting independently of direction by a foreign terrorist organization. HVEs are distinct from traditional domestic terrorists who engage in unlawful acts of violence or to intimidate civilian populations or attempt to influence domestic policy without direction from or influence from a foreign actor.

<sup>†</sup> (U//FOUO) DHS defines domestic terrorism as any kind of act of unlawful violence that is dangerous to human life or potentially destructive of critical infrastructure or key resources committed by a group or individual based and operating entirely within the United States or its territories without direction or inspiration from a foreign terrorist group. This act is a violation of the criminal laws of the United States or of any state or other subdivision of the United States and appears to be intended to intimidate or coercion, or to affect the conduct of a government by mass destruction, assassination, or kidnapping. A domestic terrorist differs from an HVE in that the former is not inspired by and does not take direction from a foreign terrorist group or foreign power.

(U) **LAW ENFORCEMENT SENSITIVE:** The information marked (U//LES) in this document is the property of the Wisconsin Statewide Information Center (WSIC) and may be distributed within the Federal Government (and its contractors), US intelligence, law enforcement, public safety or protection officials, and individuals with a need to know. Distribution beyond these entities without WSIC's authorization is prohibited. Precautions should be taken to ensure this information is stored and/or destroyed in a manner that precludes unauthorized access. Information bearing the LES caveat may not be used in legal proceedings without first receiving authorization from the originating agency. [Recipients are prohibited from subsequently posting the information marked LES on a website on an unclassified network.]

(U) **Warning:** This document contains UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO) information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). State and local homeland security officials may not share this document with critical infrastructure and key resource personnel or private sector security officials without further approval from DHS.

(U) This product contains US person information that has been deemed necessary for the intended recipient to understand, assess, or act on the information provided. It has been highlighted in this document with the label **USPER** and should be handled in accordance with the recipient's intelligence oversight and/or information handling procedures.

**(U//FOUO) “Going Dark” – The Rise of Covert Communications Platforms**

(U) In October 2014, FBI Director James B. Comey<sup>USPER</sup> discussed the current state of law enforcement abilities to leverage communication technology in front of an audience at the Brookings Institution. Director Comey stated:

*(U) Unfortunately, the law hasn't kept pace with technology, and this disconnect has created a significant public safety problem. We call it “Going Dark,” and what it means is this: Those charged with protecting our people aren't always able to access the evidence we need to prosecute crime and prevent terrorism even with lawful authority. We have the legal authority to intercept and access communications and information pursuant to court order, but we often lack the technical ability to do so.<sup>1</sup>*

(U//FOUO) Covert messaging applications are fueling the “Going Dark” trend. Commercially available secure communication platforms are not a new concept. Blackberry Messenger, a PIN-to-PIN messaging service available only on Blackberry devices, was touted as an early solution for secure corporate communications. Between 2009 and 2011, messaging apps such as WhatsApp and Kik were introduced as cross-platform, over-the-top (OTT) messaging platforms.<sup>\*,†</sup> Apple<sup>USPER</sup> responded to the growing popularity of these applications by releasing iMessage on iOS devices in 2012, which featured Wi-Fi messaging and end-to-end encryption. Other secure messaging apps, such as Wickr, Telegram, TextSecure, and surespot, were subsequently released.<sup>2</sup>

(U//FOUO) Increased public awareness of government surveillance has contributed to the rising consumer demand for covert messaging apps. This trend led software developers to use advancing technologies to make these apps more user-friendly than previous releases. Technological knowledge barriers that once prevented the average citizen from securing his/her communications have fallen, and covert messaging apps have gone mainstream.<sup>3</sup>

(U//LES) Criminals and violent extremists have taken notice of the ever-expanding technologies available to conceal their interactions and evade detection by law enforcement.<sup>4,5,6</sup> In his June 3, 2015 testimony before the House Committee on Homeland Security, FBI Assistant Director Michael Steinbach<sup>USPER</sup> pointed to “mobile apps like Kik and WhatsApp as well as data-destroying apps like Wickr and surespot” as the burgeoning apps of choice for Islamic State of Iraq and the Levant (ISIL) interactions.<sup>7</sup>

(U//FOUO) With the field of covert messaging platforms continually diversifying, it is important to note the subtle differences between the apps and what they offer. Covert messaging software can encompass off-network messaging and/or secure (encrypted) messaging.

**(U//FOUO) Off-Network Messaging**

(U//FOUO) Off-network communication technology is popular for messaging apps because it does not rely on a mobile phone's cellular data plan to function. Instead, users are able to send and receive messages from their phone using a Wi-Fi network when cellular networks are not available or if a user wants to communicate without using cellular company infrastructure. Messages do not register on the user's phone plan and are not discoverable by legal demand served on the mobile phone carrier (for example, search warrants or court orders; check with your local jurisdiction to determine what

<sup>\*</sup> (U//FOUO) Cross-platform in this context refers to the ability of software to function identically on different operating systems—Apple's iOS, Google's Android, Microsoft's Windows, etc.

<sup>†</sup> (U//FOUO) Over-the-top content refers to the delivery of any content (audio, video, etc.) from a third party service provider.

constitutes a valid legal demand). However, the data may be available through serving legal demand on software application providers. Other devices, such as tablets, can also be used to communicate through off-network messaging platforms.<sup>8</sup>

#### (U) Encryption Basics

*(U//FOUO) Encrypted communication refers to a transmission of information that is essentially scrambled with a cryptographic code so that the information is unreadable to any person without the key to the code. Unauthorized parties can still intercept encrypted information, but the message that they receive will be nearly indecipherable.*

*(U//FOUO) An important part of the encryption protocol is where the key data for decryption is stored. Companies that store the decryption key for messages on their servers run the risk of a data compromise if a hacker is able to retrieve the decryption key from their servers and decrypt the messages.<sup>9</sup>*

*(U//FOUO) One of the most common encryption schemas is the asymmetric pair exchange. A person, call him Andrew, is assigned a Public Key, which is a long string of numbers that the person will display publically. If another person, Barb, wants to send Andrew secured information, she will use Andrew's Public Key to encrypt the data. When Andrew receives the message, he will use the mathematically corresponding Private Key that is assigned to him to decrypt the message. Only the person with the corresponding Private Key to the encrypted message's Public Key will be able to get the scrambled message back to its intended form, so it is imperative that Private Keys are not shared.*

*(U//FOUO) Most secure messaging apps are now promising "end-to-end encryption." End-to-end encryption is more secure because the Private Key pairs used during the communication remain on the user's devices and are not uploaded to the app's servers. No "backdoors" into the secure messaging services can be installed because the information passing through the services is indecipherable without the Private Keys stored on the participating users' devices.*

*(U//FOUO) To combat the problem of sophisticated hackers attempting to mathematically break Public Key encryption, more services have begun to implement Forward Secrecy in their protocols. Forward Secrecy protocols feature Public/Private Key pairs that are created for each session; these pairs are never stored or reused. If an attacker were to break the encryption code, the attacker would only have access to the information exchanged in that session alone. No future or historical information would be available due to the reassignment of keys.*

#### (U) Secure (Encrypted) Messaging

(U//FOUO) Secure messaging offers even more safeguards against message interception. These apps contain some level of encryption for any communications sent using the service. Encryption protocols range from the most basic forms of encryption to high-level proprietary protocols designed by some of the world's leading cryptographers.<sup>10</sup>

(U//FOUO) Secure messaging apps have a reputation to uphold within their user community that the apps' services are secure, encrypted, and free from government intrusion. Some companies have gone so far as to promote the use of a "warrant canary" to inform users whether or not a secret government subpoena has been filed on the company.<sup>11</sup>

- (U//FOUO) Wickr<sup>USPER</sup> places its warrant canary in their annual transparency reports. The warrant canary states, "As of the date of this report, Wickr has not been required by a FISA request to keep any secrets that are not in this transparency report as part of a national security order."<sup>12</sup> Wickr alerted users in its blog that if the warrant canary disappears in its report then things "will have shifted."<sup>13</sup>
- (U//FOUO) In late 2013, Apple published its first transparency report and it contained its warrant canary: "Apple has never received an order under Section 215 of the USA Patriot Act. We would expect to challenge such an order if served on us." The next two transparency reports that Apple published no longer featured the warrant canary, which led many people to speculate that Apple may have been served federal legal demand.<sup>14</sup>

- (U//FOUO) Bloggers can also act as an unofficial warrant canary for companies. A tech blogger regularly e-mails 2fours<sup>USPER</sup>, surespot's parent company, questioning whether or not they have received requests to cooperate with a government agency and if the company has ever received a National Security Letter. In May 2014, 2fours replied that the answer to all of the blogger's questions was no. In November 2014, the blogger repeated the e-mail, and 2fours responded that they had received an e-mail regarding how one could serve a subpoena to 2fours. In April 2015, the blogger re-sent the questions and received no reply back from the company.<sup>15</sup>

### (U//FOUO) Common Covert Messaging Apps

(U//FOUO) Like many commercial products, covert messaging apps are evaluated in online buyers' guides and forums.<sup>16</sup> The most highly regarded platforms are discussed below. Unless otherwise noted, the apps are available for both iOS and Android users.

- (U//FOUO) **KIK** – First released in October 2010, the Kik Messenger app allows users to share voice, text, images, and other content. Kik Messenger works through a unique Kik ID that allows users to contact each other regardless of whether or not they are in the recipient's contact network. All the user has to do is publicize his/her Kik name, and any other Kik user may contact them.<sup>17</sup> Due to its popularity with teens and tweens, sexual predators have often used Kik. To combat the pervasive nature of the child exploitation threat over its software, Kik partnered with Microsoft's PhotoDNA software that will help block the distribution of child pornography over the app. Kik recently surpassed 200 million users.<sup>18</sup>



- (U//FOUO) **WHATSAPP** – With approximately 800 million users, WhatsApp is the most popular messaging service available. The company is based in Mountainview, CA and Facebook<sup>USPER</sup> acquired WhatsApp<sup>USPER</sup> in early 2014.<sup>19</sup> WhatsApp added TextSecure end-to-end encryption technology to their services at the end of 2014. However, a recent study showed that iOS devices do not support the TextSecure protocol, and WhatsApp messages sent or received from an iPhone are not encrypted and more vulnerable to interception.<sup>20</sup>



- (U//FOUO) **SURESPOT** – First released in December 2014, surespot is a secured messaging app that allows for voice and text messaging. It does not support group messaging or file attachments other than photos. Surespot is entirely open source software, so the users are able to review the code and security protocols that are used.<sup>21</sup> Surespot is owned and developed by 2fours, a company based out of Boulder, CO. Surespot has less than 500,000 downloads through the Google Play store.<sup>22</sup>



- (U//FOUO) **TELEGRAM** – The Telegram message app was first released in August 2013. Telegram messaging service is available for phones and personal computers and is mostly cloud-based. The Durov brothers, the founders of Russian VK, developed the app, and the company is based in Berlin, Germany. Telegram has over 50 million active users and exchanges nearly 1 billion messages a day.<sup>23</sup>



- (U//FOUO) **WICKR** – The Wickr app was first released in June 2012; it is available on Android and iOS platforms as well as Windows desktop. The Wickr app supports the transmission of text, video, audio or images. Users are able to edit images that are





sent through the app. Wickr is based out of San Francisco and has over a million downloads.<sup>24</sup>

**(U//FOUO) SCRAMBL3** – The newest secure messaging application, Scrambl3, was released in



early June 2015. Scrambl3 is currently only available on Android devices and allows for text and voice communication. Scrambl3 was developed from the last NSA standards to protect Top Secret classified communications.<sup>25</sup> US Mobile<sup>USPER</sup>, whose headquarters is in Irvine, CA, created the app. Since the app is newly released, Scrambl3 has less than 5,000 downloads from the Google Play store. Scrambl3 is not yet available on iOS devices.<sup>26</sup>

- **(U//FOUO) THREEMA** – The Threema app was released in late 2012, and it supports text, voice and multimedia messaging. Threema GmbH developed the software.<sup>27</sup> All of the company's servers are located in Switzerland. Threema has less than 5 million downloads in the Google Play store.



- **(U//FOUO) SILENT CIRCLE** – Mike Janke<sup>USPER</sup> and Phil Zimmerman<sup>USPER</sup> founded the Silent Circle company in 2012. Zimmerman created Pretty Good Privacy (PGP), a widely used e-mail encryption software program. Silent Phone, released in late 2012, offers encrypted video and voice for paid subscribers. The company followed by releasing Silent Text, which offers encrypted data transfers (text, images, audio) between parties. In June 2014, Silent Circle and Geeksphone teamed up to release the Blackphone, an Android-based smartphone operating Silent Circle's full suite of privacy products and several other privacy-focused features. The company will release Blackphone 2 in September of this year.<sup>28</sup> Silent Circle is based out of Switzerland, and the apps have nearly a million downloads between iOS and Android platforms. Dutch mobile network provider KPN recently partnered with Silent Circle to become the first telecom provider in the world to offer customers encrypted communications services using Silent Text and Silent Phone.<sup>29</sup>



(U//FOUO) See Appendix A for further details on covert messaging apps.

**(U//FOUO) Terrorists and Criminals Seek Out Secure Communications Services**

(U//FOUO) While ISIL has been prolific in their use of social media to help radicalize and recruit individuals, ISIL members and their supporters are learning the risks and vulnerabilities that arise when relying so heavily on publicly available technology.<sup>30</sup> ISIL social media accounts now regularly feature guidance to their followers on how best to obfuscate communications. Recommendations now include setting up Virtual Private Networks (VPNs) when browsing the internet to conceal Internet protocol (IP) address and cookie information, as well as encrypting any e-mails that are sent.<sup>31</sup> ISIL leaders have become so concerned about surveillance and intelligence collection that they have banned certain devices and technologies on the battlefield. According to media reporting, Apple products are forbidden in their caliphate, as ISIL believes Android devices are more secure.<sup>32</sup>

(U//FOUO) As the number of successful counterterrorism interdiction efforts continues to rise, violent extremists are increasingly turning to more secure methods of interaction. Media reporting highlights specific communications vulnerabilities, and violent extremist forums regularly discuss the best covert communications options.<sup>33</sup>

- (U//FOUO) On June 8, 2015, Belgian authorities arrested 16 conspirators in several anti-terror raids. Belgian law enforcement officials told the media that they had been monitoring the suspects' communications over WhatsApp.<sup>34</sup>
- (U//FOUO) On May 27, 2015, probably deceased ISIL fighter Junaid Hussain tweeted publically that any individuals interested in waging lone offender attacks should contact him using the messaging application surespot. Hussain stated that "these days u don't even need to go abroad for training you can be taught & assisted online via 200 percent secure methods."<sup>35</sup>
- (U//FOUO) In November 4, 2014, a follower of ISIL on Twitter<sup>USPER</sup>, posted publically that individuals should "NOT use KIK Messenger when chatting about sensitive Jihadi stuff" because it was not secure. Following his post, there was a discussion among his followers of apps that were preferred and known to be secure.<sup>36</sup>

(U//LES) Internationally-based violent extremists are not the only ones who have found use for secure messaging apps. A body of open source and law enforcement reporting notes that drug trafficking organizations, HVEs, and militia extremists are using the apps to evade surveillance.<sup>37</sup>

- (U) Rafael Caro Quintero, former leader of the Guadalajara cartel, used WhatsApp to send video messages to leaders of the New Generation Jalisco cartel according to media reporting in July 2015.<sup>38</sup>
- (U//LES) Drug trafficking organizations are using Silent Circle products to encrypt their communications. Law enforcement reports Silent Circle is being utilized in Atlanta, Dallas, Denver, Philadelphia, and San Francisco as of February 2015.<sup>39</sup>
- (U) Ali Shukri Amin<sup>USPER</sup>, a 17-year-old from Virginia, pled guilty to providing material support and resources to ISIL. Court documents filed on 11 June 2015 describe the teen's use of the surespot app to organize the travel of a supporter to Syria.<sup>40</sup>
- (U//LES) Militia extremists in Utah are telling members to use secure messaging services like Wickr to discuss surveillance and group membership, according to analysis by the Utah Statewide Information & Analysis Center in April 2015.<sup>41</sup>

### (U//LES) Law Enforcement Implications for Covert Messaging Apps

(U//FOUO) Law enforcement investigators will be able to send legal demand to messaging software companies based in the United States. However, the information that is returned may not be useful, as most of these companies do not store message content on their servers. If the company stores message content on its servers, it is likely that the content that is returned will be indecipherable without the user's key, typically stored on the user's device. Depending on the app, identifying account information may or may not be stored with the company, so it is imperative for the investigator to visit the specific app's website to determine what the company can or cannot produce. Most importantly, nearly all of the companies have data request disclosure policies that will notify the user if a legal demand is submitted for the individual's account information. It is imperative that investigators use language in their legal demand to legally prohibit the company from doing so ("gag order" language).

(U//FOUO) If the company is based outside the United States, an investigator must take special considerations when filing legal demand to ensure compliance. In some cases, a Mutual Legal Assistance Treaty (MLAT) between the US Government and the company's host government is typically required for any legal demands to be served on the company.<sup>42</sup> Kik Messenger, based out of Canada, cautions agencies that a MLAT may be required to obtain any user data from Kik.<sup>43</sup>

(U//FOUO) Since the message content in most secure messaging apps is saved only on the device, apps like Threema recommend creating an identity backup of the phone using the device's backup system.<sup>44</sup> If a backup is created, it could be stored in the device's cloud storage (e.g., iCloud and OneDrive), which means that it may be accessible to law enforcement if the investigator chooses to subpoena any cloud accounts for the subject of the investigation. The identity backups look different for each app, but the investigator may be able to see the chat messages and contact list, depending on the app and user settings.<sup>45</sup>

(U//LES) Forensic examination of the subject's device may find conversation artifacts depending on the app the subject used. However, if the device itself has a passcode or is encrypted, the forensic analyst will have a greatly reduced chance of recovering any evidence as forensic examination technology has limited capability for analyzing locked devices. Forensic examiners stress the importance of interviewing the subject and asking for any device passwords and any passwords or keys associated with the apps installed on the subject's phone.<sup>46</sup>

## (U) Outlook

(U//LES) The type of app selected by malicious actors is often influenced by both security features and the population using the app. Sophisticated organizations typically use apps that are both off-network and encrypted. Other criminal actors like human trafficking rings or child predators may use platforms like Kik, which is not encrypted, because the app's use among teens is so high. Understanding how covert messaging applications work and the different features of secure or off-network technology is crucial for law enforcement investigators. Often there will be little information that can be retrieved from serving legal demand on these communication software providers. However, the ability to recognize that a subject is using a covert app can lead to more informed interviews of the subject and any conspirators. Awareness also enables a more focused forensic examination of any devices seized.<sup>47</sup>

(U//LES) Knowledge that the subject of a law enforcement investigation is using covert messaging may also enable decisions about alternative investigative techniques such as confidential informants or undercover operations.

## (U//FOUO) Appendix A – Covert Messaging Application Attributes

UNCLASSIFIED//FOR OFFICIAL USE ONLY

App	Encryption/Key Assignment	Message/Data Storage and Deletion	Registration and Retention
<b>Kik</b>	None	Messages are only stored on the user's device. Message artifacts can be found forensically, even after deletion.	Register with unique Kik username. The phone number of the device is not stored or accessible by Kik.
<b>WhatsApp</b>	End-to-end encryption using TextSecure encryption on Android platform. Only stores keys on the user's device. Assigns new key with every message.	Messages are stored on the user's device. All messages pass through WhatsApp servers. Files sent through messaging (images, videos) are stored for a short period of time after delivery. <sup>48</sup>	Uses device phone number to route chats and calls to user. Uses device's phone book to find other registered users with whom to chat.
<b>surespot</b>	End-to-end encryption. Key pairs are assigned at registration, tied to username. Users can regenerate their keys at any time. App allows key verification between chat participants.	Message data and keys are encrypted and stored on the device. Data can be decrypted with user's password. Message deleted from sender's phone will be deleted on the recipient's phone and surespot server as well. App also runs cache processes that will leave significant artifacts that can be found during forensic examination.	Register with unique surespot username and password. Passwords can never be reset or recovered. Users can create multiple identities to use on the same device.
<b>Silent Circle</b> <b>Silent Phone</b> <b>Silent Text</b>	Uses Silent Circle Instant Messaging Protocol (SCIMP) with end-to-end encryption. Practices forward secrecy by assigning distinct keys for each message to both users. Keys are erased from memory.	Silent Text has a "Burn Notice" feature that allows users to decide how long a message can be viewed before it is deleted from both sending and receiving devices.	Paid subscriptions to Silent Text and Silent Phone required; subscriber credit card data is held by Stripe <sup>USPER</sup> . Silent Circle retains username and encrypted password.
<b>Telegram</b>	End-to-end encryption only on "Secret Chat" feature. Secret Chat has rotating key protocol that discards old previously used keys. App allows key verification between chat participants.	Users can elect to have messages in Secret Chat self-destruct after so many seconds. Messages deleted from sender's phone will be deleted on the recipient's phone. All messages, including Secret Chats, are stored in the device in plain text. <sup>49</sup> Forensic examination will likely produce Secret Chats and any deleted messages.	Account is tied to device phone number. Users can also establish a public username if they want to be searchable.
<b>Wickr</b>	End-to-end encryption. Practices forward secrecy by assigning new keys for each message.	Users can set their message to last between three seconds and six days. Once messages are deleted, they are forensically wiped from the phone. "Secure Shredder" feature runs in the background and wipes previously deleted information, making it unattainable to forensic examination. Removes all metadata from messages and media.	Device registration is encrypted. Unique Device Identifier is never uploaded to Wickr's servers, so user is anonymous.
<b>Scrambl3</b>	Employs encryption protocols and then places that information in "Dark Internet Tunnels" of proprietary encryption protocols.	No information currently available, as the app has just been released.	No information currently available, as the app has just been released.
<b>Threema</b>	End-to-end encryption. Key pairs are assigned at registration and regenerated whenever the app is launched.	No information available.	No phone number is required at registration. However, it is recommended that the user links the Threema ID to the phone number in order to be discoverable to contacts.



**(U) DHS I&A Perspective**

(U//FOUO) DHS I&A assesses that growing concerns regarding the privacy of user data and the perceived spying by US law enforcement and the US Government are driving ordinary citizens as well as criminal elements to more secure or anonymizing methods of communication. The increasing market demand for secure services will continue to spark the startup of anonymization companies and the development of new techniques to counter law enforcement efforts.

- » (U) A Pew Research Center poll from late 2013 revealed that as many as eighty-six percent of Internet users have taken steps online to remove or mask their digital footprints—ranging from clearing cookies to encrypting their e-mail, from avoiding using their name to using virtual networks that mask their IP address. Fifty-five percent of Internet users have taken steps to avoid observation by specific people, organizations, or the government.<sup>50</sup>
- » (U) Encrypted Internet traffic is surging worldwide, according to data published by Canadian broadband management company Sandvine. After the public accusations of US Government spying in 2014, the bandwidth consumed by encrypted traffic doubled in North America; in Europe and Latin America the share of encrypted traffic quadrupled.<sup>51,52</sup>

(U//FOUO) Technology savvy criminals, driven by the fear of government tracking and surveillance, are likely to increase their use of anonymizing applications such as The Onion Router (TOR) and unindexed “invisible” sections of the Internet called the Deep Web. Use of these services would almost certainly impair law enforcement efforts to identify malicious actors.

**(U//FOUO) TOR and the Deep Web**

*(U) TOR is free software for enabling anonymous communication. TOR directs Internet traffic through a free, worldwide, volunteer network consisting of more than six thousand relays to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis.<sup>53</sup>*

*(U) The Deep Web is an unindexed section of the Internet. Deep Web pages operate just like any other site online, but they are constructed so that their existence is invisible to web crawlers such as search engines. The Deep Web is filled with content and sites of a nefarious nature that are only accessible via tools like TOR.<sup>54</sup>*

(U//FOUO) DHS I&A further assesses that HVEs will likely continue to use covert messaging applications to plan both travel and Homeland attacks. Due to the security restrictions of such apps, it is increasingly imperative that bystanders—to include parents, teachers, and community members—remain aware of possible signs of radicalization and mobilization to violence and report concerns to the appropriate authorities.

(U//FOUO) Comments, requests, or shareable intelligence may be directed to the Wisconsin Statewide Information Center at (888) 324-9742 or [wsic@doj.state.wi.us](mailto:wsic@doj.state.wi.us).

**(U//FOUO) Source Summary Statement**

(U//FOUO) This report was drawn from government documents, law enforcement reporting, and open source information. In addition, the daily criminal investigation case support duties of analysts assigned to the WSIC Intelligence & Analysis Unit (IAU) informed this product. We have **high confidence** in the validity of all sources used and our review of covert messaging technology. We have **medium confidence** in our characterization of violent extremist and criminal use of covert messaging technologies. This is due to the emergent and rapidly changing nature of specific technologies discussed and the paucity of associated human source reporting.

**(U) Report Suspicious Activity**

**(U) To report suspicious activity, law enforcement, Fire-EMS, private security personnel, and emergency managers should follow established protocols; all other personnel should call 911 or contact local law enforcement.** Suspicious activity reports (SARs) will be forwarded to the appropriate fusion center and FBI Joint Terrorism Task Force for further action. For more information on the Nationwide SAR Initiative, visit <http://nsi.ncirc.gov/resources.aspx>.

**(U) Tracked by:** HSEC-8.2.2, HSEC-8.2.4, HSEC-8.7.1, HSEC-8.7.2.12, HSEC-8.8.1, HSEC-8.8.3

<sup>1</sup> (U); James B. Comey; FBI, Director; "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?"; 16 OCT 2014; Extracted information is UNCLASSIFIED; Overall speech was UNCLASSIFIED; Remarks as delivered at the Brookings Institution.

<sup>2</sup> (U); Molly Wood; The New York Times; "Can you trust 'secure' messaging apps?"; 19 MAR 2014; [http://bits.blogs.nytimes.com/2014/03/19/can-you-trust-secure-messaging-apps/?\\_r=0](http://bits.blogs.nytimes.com/2014/03/19/can-you-trust-secure-messaging-apps/?_r=0); accessed 21 JUL 2015; (U).

<sup>3</sup> (U); Ellen Nakashima; The Washington Post; "Proliferation of New Online Communications Services Poses Hurdles"; 26 JUL 2014; [www.washingtonpost.com/world/national-security/proliferation-of-new-online-communications-services-poses-hurdles-for-law-enforcement/2014/07/25/645b13aa-0d21-11e4-b8e5-d0de80767fc2\\_story.html](http://www.washingtonpost.com/world/national-security/proliferation-of-new-online-communications-services-poses-hurdles-for-law-enforcement/2014/07/25/645b13aa-0d21-11e4-b8e5-d0de80767fc2_story.html); accessed on 21 JUL 2015; (U).

<sup>4</sup> (U); WSIC Intelligence & Analysis Unit; Meetings; 2014; 2015; (U); Weekly Analyst Meeting-Criminal Case Support Discussions; Extracted information is U//LES; Overall meeting discussions were U//LES.

<sup>5</sup> (U//LES); FBI; SIR-00016284722; 26 FEB 2015; DOI UNK; (U//LES); Communications Security Measures of a Western US-Based Militia Extremist Group; Extracted information is U//LES; Overall document classification is U//LES.

<sup>6</sup> (U); Ellen Nakashima; The Washington Post; "Proliferation of New Online Communications Services Poses Hurdles"; 26 JUL 2014; [www.washingtonpost.com/world/national-security/proliferation-of-new-online-communications-services-poses-hurdles-for-law-enforcement/2014/07/25/645b13aa-0d21-11e4-b8e5-d0de80767fc2\\_story.html](http://www.washingtonpost.com/world/national-security/proliferation-of-new-online-communications-services-poses-hurdles-for-law-enforcement/2014/07/25/645b13aa-0d21-11e4-b8e5-d0de80767fc2_story.html); accessed on 21 JUL 2015; (U).

<sup>7</sup> (U); Michael Steinbach; FBI, Assistant Director, Counterterrorism Division; Terrorism Gone Viral: The Attack in Garland, Texas and Beyond; Statement Before the House Homeland Security Committee; 3 JUN 2015; Extracted information is UNCLASSIFIED; Overall testimony was UNCLASSIFIED.

<sup>8</sup> (U); Susan Kantra; USA Today; "Free messaging apps can help you stop paying for texts"; 15 JUN 2013; <http://www.usatoday.com/story/tech/personal/2013/06/15/techlicious-text-message-alternatives/2423169/>; accessed on 21 JUL 2015; (U).

<sup>9</sup> (U); Andy Greenberg; WIRED; "Hacker lexicon: What is end-to-end encryption?"; 25 NOV 2014; <http://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/>; accessed 21 JUL 2015; (U).

<sup>10</sup> (U); Neal Ungerleider; Fast Company; "Phil Zimmerman's Silent Circle builds a secure, seductive fortress around your smartphone"; 5 OCT 2012; <http://www.fastcompany.com/3001938/phil-zimmermanns-silent-circle-builds-secure-seductive-fortress-around-your-smartphone>; accessed on 21 JUL 2015; (U); Blog.

<sup>11</sup> (U); Zack Whittaker; ZDNet; "How tech companies use warrant canaries to secretly communicate with you"; 5 MAR 2015; <http://www.zdnet.com/article/warrant-canary/>; accessed 21 JUL 2015; (U).

<sup>12</sup> (U); WICKR; "Wickr Transparency Report 2015"; <https://wickr.com/category/transparency-report/>; accessed on 21 JUL 2015; (U).

<sup>13</sup> (U); WICKR; "Wickr Transparency Report 2015"; <https://wickr.com/category/transparency-report/>; accessed on 21 JUL 2015; (U).

- <sup>14</sup> (U); Zack Whittaker; ZDNET; "Apple omits 'warrant canary' from latest transparency reports; Patriot Act data demands likely made"; 18 SEPT 2014; <http://www.zdnet.com/article/apple-omits-warrant-canary-from-latest-transparency-reports-patriot-act-data-demands-likely-made/>; accessed 21 JUL 2015; (U).
- <sup>15</sup> (U); George Maschke; Antipolygraph.org News; "Developer's silence raises concern about Surespot Encrypted Messenger"; 7 JUN 2015; <https://antipolygraph.org/blog/2015/06/07/developers-silence-raises-concern-about-surespot-encrypted-messenger/>; accessed on 21 JUL 2015; (U); Blog.
- <sup>16</sup> (U); The Electronic Frontier Foundation; "Secure messaging scorecard"; 12 JUN 2015; <https://www.eff.org/secure-messaging-scorecard>; accessed on 21 JUL 2015; (U) Blog.
- <sup>17</sup> (U); Kik Help Center; "Frequently Asked Questions"; <https://kikinteractive.zendesk.com/forums>; 2013; accessed on 21 JULY 2015; (U).
- <sup>18</sup> (U); Shane Dingman; The Globe and Mail; "For fast-growing chat apps like Waterloo's Kik, child exploitation a pervasive threat," 16 MAR 2015; <http://www.theglobeandmail.com/technology/for-fast-growing-chat-apps-child-predators-are-a-pervasive-threat/article23485785/>; accessed on 21 JUL 2015; (U).
- <sup>19</sup> (U); WhatsApp; "Contact Us"; 2015; <https://www.whatsapp.com/contact/>; accessed on 21 JUL 2015; (U).
- <sup>20</sup> (U); Fabian A. Scherschel; c't magazine; "Keeping Tabs on WhatsApp's Encryption," 30 APR 2015; <http://www.heise.de/ct/artikel/Keeping-Tabs-on-WhatsApp-s-Encryption-2630361.html>; accessed on 21 AUG 2015; (U).
- <sup>21</sup> (U); Google Play; "surespot encrypted messenger"; 12 DEC 2014; <https://play.google.com/store/apps/details?id=com.twofours.surespot>; accessed 21 JUL 2015; (U).
- <sup>22</sup> (U); Google Play; "surespot encrypted messenger"; 12 DEC 2014; <https://play.google.com/store/apps/details?id=com.twofours.surespot>; accessed 21 JUL 2015; (U).
- <sup>23</sup> (U); The Telegram Team; Telegram Blog; "Telegram reaches 1 billion daily messages"; 8 DEC 2014; <https://telegram.org/blog/billion>; accessed on 21 JUL 2015; (U) Blog.
- <sup>24</sup> (U); WICKR; "Wickr"; <https://wickr.com/>; accessed on 21 JUL 2015; (U).
- <sup>25</sup> (U); PR Newswire; "US mobile launches Scrambl3 mobile app to the public; the world's most secure cellphone service, developed for Top Secret Classified Communication, now available at Google Play Store"; 1 JUN 2015; <http://www.prnewswire.com/news-releases/usmobile-launches-scrambl3-mobile-app-to-the-public-the-worlds-most-secure-cellphone-service-developed-for-top-secret-classified-communication-now-available-at-google-play-store-300091319.html>; accessed on 21 JUL 2015; (U) Blog.
- <sup>26</sup> (U); Google Play; "Scrambl3"; 20 JUL 2015; <https://play.google.com/store/apps/details?id=com.usmobile.scrambl3>; accessed 24 AUG 2015; (U).
- <sup>27</sup> (U); Threema; "Threema. Seriously secure messaging."; <https://threema.ch/en>; accessed on 21 AUG 2015; (U).
- <sup>28</sup> (U); Silent Circle; "Silent Circle Support Center"; 2015; <https://support.silentcircle.com/>; accessed on 21 JUL 2015; (U) Blog.
- <sup>29</sup> (U); Loek Essers; PCWorld. "KPN strikes deal with Silent Circle to offer encrypted phone calls"; 19 FEB 2014; <http://www.pcworld.com/article/2099160/kpn-strikes-deal-with-silent-circle-to-offer-encrypted-phone-calls.html>; accessed on 21 JUL 2015; (U) Blog.
- <sup>30</sup> (U); Francis X. Taylor; DHS, Under Secretary, Office of Intelligence and Analysis; Terrorism Gone Viral: The Attack in Garland, Texas and Beyond; Statement Before the House Homeland Security Committee; 3 JUN 2015; Extracted information is UNCLASSIFIED; Overall testimony was UNCLASSIFIED.
- <sup>31</sup> (U); Channel 4 News; "Forget Facebook: jihadists are using different networks"; 26 NOV 2014; <http://www.channel4.com/news/islamic-state-messaging-apps-facebook-monitor-terrorism>; accessed on 21 JUL 2015; (U).
- <sup>32</sup> (U); Alessandria Masi; International Business Times; "ISIS bans Apple iPhones, iPads, iPods in the caliphate due to fears they're being tracked"; 6 FEB 2015; <http://www.ibtimes.com/isis-bans-apple-iphones-ipads-ipods-caliphate-due-fears-theyre-being-tracked-1807006>; accessed on 21 JUL 2015; (U) Blog.
- <sup>33</sup> (U//FOUO); Intelligence Watch and Warning, Current Intelligence Division, Department of Homeland Security; E-mail; 13 FEB 2015; DOI 5 FEB 2015; (U//FOUO); "Hijrah (2015) to the Islamic State"--Posted to Internet; Extracted information is UNCLASSIFIED; Overall document classification U//FOUO; Hijrah (2015) to the Islamic State pdf attached to e-mail.
- <sup>34</sup> (U); BBC News; "Belgium arrests in anti-terror raids targeting Chechens"; 8 JUN 2015; <http://www.bbc.com/news/world-europe-33046258>; accessed 21 JUL 2015; (U) Blog.
- <sup>35</sup> (U//FOUO); OSC; EUL2015052752693374; 27 MAY 2015; DOI MAY 2015; British ISIL Fighter Urges Muslims in West To Perpetrate 'Lone Wolf' Attacks; Extracted information is UNCLASSIFIED; Overall document classification U//FOUO.
- <sup>36</sup> (U); The Cyber & Jihad Lab; "ISIS follower on Twitter warns against using Kik Messenger Service 'when chatting about sensitive jihadi stuff'; recommends other technologies"; 5 NOV 2014; <http://cjlaboratory.org/lab-projects/tracking-jihadi-terrorist-use-of-social-media/isis-follower-on-twitter-warns-against-using-kik-messenger-service-when-chatting-about-sensitive-jihadi-stuff-recommends-other-technologies/>; accessed on 21 JUL 2015; (U).
- <sup>37</sup> (U//LES); FBI; "Increasing Availability and Drug Traffickers' Adoption of Encrypted Mobile Messaging Applications Threaten Law Enforcement Collection"; 11 APR 2014; pg 1; (U//LES).

- <sup>38</sup> (U); Fusion; "Mexican millennials at the forefront of drug war intelligence"; <http://fusion.net/story/28864/mexican-millennials-at-the-forefront-of-drug-war-intelligence>; accessed on 21 JUL 2015; (U).
- <sup>39</sup> (U//LES); DEA; "DEA-HOU-BUL-073-15 - Silent Circle: Another Encrypted Option Emerges in the Houston Division"; FEB 2015; pg 1; (U//LES).
- <sup>40</sup> (U); US District Court, Eastern District of Virginia, Alexandria Division; "United States of America, Plaintiff versus ALI SHUKRI AMIN; 11 JUN 2015; pg 4.
- <sup>41</sup> (U//LES); Utah Statewide Information & Analysis Center; "Militia Extremists Begin Intel Collection in State of Utah"; 28 APR 2015; pg 2; (U//LES).
- <sup>42</sup> (U); Orin Kerr; The Washington Post; "What legal protections apply to e-mail stored outside the U.S.?"; 7 JUL 2014; <https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/07/07/what-legal-protections-apply-to-e-mail-stored-outside-the-u-s/>; accessed on 21 JUL 2015; (U) Blog.
- <sup>43</sup> (U); Kik; "Law Enforcement Guide"; 13 NOV 2014; <https://kiklawenforcement.zendesk.com/hc/en-us/articles/203419779-Download-our-Guide-for-Law-Enforcement>; accessed on 21 JUL 2015; (U).
- <sup>44</sup> (U); Threema; "Threema FAQ"; 2015; <https://threema.ch/en/faq>; accessed on 21 JUL 2015; (U) Blog.
- <sup>45</sup> (U); Threema; "Threema FAQ"; 2015; <https://threema.ch/en/faq>; accessed on 21 JUL 2015; (U) Blog.
- <sup>46</sup> (U); Mark Howard; Senior Digital Forensics Analyst, Wisconsin Department of Justice; 16 JUN 2015; (U//LES); "Observations on Encrypted Messaging Apps and Forensic Examinations"; Extracted information is U; Overall document classification is U//LES; E-mail.
- <sup>47</sup> (U); WSIC Intelligence & Analysis Unit; Meetings; 2014; 2015; (U); Weekly Analyst Meeting-Criminal Case Support Discussions; Extracted information is U//LES; Overall meeting discussions were U//LES.
- <sup>48</sup> (U); Kids and Teens Online; "Where do pictures and files we send using Whatsapp end up?"; 10 OCT 2013; <http://kidsandteensonline.com/2013/10/10/where-do-pictures-and-files-we-send-using-whatsapp-end-up/>; accessed 21 JUL 2015; (U) Blog.
- <sup>49</sup> (U); Zuk Avraham; Zimperium Mobile Security; "Telegram app store secret-chat messages in plain-text database"; 23 FEB 2015; <http://blog.zimperium.com/telegram-hack>; accessed 21 JUL 2015; (U); Blog.
- <sup>50</sup> (U) Pew Internet and American Life Project; "Anonymity, Privacy, and Security Online"; <http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/>; accessed 24 AUG 2015.
- <sup>51</sup> (U) Sandvine; "Global Internet Phenomena Report – 2H 2014"; <https://www.sandvine.com/downloads/general/global-internet-phenomena/2014/2h-2014-global-internet-phenomena-report.pdf>; Accessed 24 AUG 2015.
- <sup>52</sup> (U) TorrentFreak; "Encrypted Internet Traffic Surges in a Year, Research Shows"; 14 MAY 2014; <https://torrentfreak.com/encrypted-internet-traffic-surges-140514/>; accessed 28 SEP 2015; (U).
- <sup>53</sup> (U) Trend Micro; "The Deep Web: Anonymizing Technology for the Good...and the Bad?"; 01 JUN 2015; <http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-deep-web-anonymizing-technology-good-and-bad>; accessed 28 SEP 2015; (U).
- <sup>54</sup> (U) Trend Micro; "The Deep Web: Anonymizing Technology for the Good...and the Bad?"; 01 JUN 2015; <http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-deep-web-anonymizing-technology-good-and-bad>; accessed 28 SEP 2015; (U).





# Homeland Security

Office of Intelligence and Analysis

## Customer Feedback Form

Product Title: (U//FOUO) Going Dark – Covert Messaging Applications and Law Enforcement Implications

1. Please select partner type: and function: 

2. What is the highest level of intelligence information that you receive?

3. Please complete the following sentence: "I focus most of my time on:"

4. Please rate your satisfaction with each of the following:

	Very Satisfied	Somewhat Satisfied	Neither Satisfied nor Dissatisfied	Somewhat Dissatisfied	Very Dissatisfied	N/A
Product's overall usefulness	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Product's relevance to your mission	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Product's timeliness	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Product's responsiveness to your intelligence needs	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

5. How do you plan to use this product in support of your mission? (Check all that apply.)

- |  |   |
|--|---|
| <input type="checkbox"/> Drive planning and preparedness efforts, training, and/or emergency response operations | <input type="checkbox"/> Initiate a law enforcement investigation       |
| <input type="checkbox"/> Observe, identify, and/or disrupt threats   | <input type="checkbox"/> Initiate your own regional-specific analysis   |
| <input type="checkbox"/> Share with partners   | <input type="checkbox"/> Initiate your own topic-specific analysis      |
| <input type="checkbox"/> Allocate resources (e.g. equipment and personnel)                                       | <input type="checkbox"/> Develop long-term homeland security strategies |
| <input type="checkbox"/> Reprioritize organizational focus   | <input type="checkbox"/> Do not plan to use                             |
| <input type="checkbox"/> Author or adjust policies and guidelines  | <input type="checkbox"/> Other: <input type="text"/>                    |

6. To further understand your response to question #5, please provide specific details about situations in which you might use this product.

7. What did this product not address that you anticipated it would?

8. To what extent do you agree with the following two statements?

	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree	N/A
This product will enable me to make better decisions regarding this topic.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
This product provided me with intelligence information I did not find elsewhere.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

9. How did you obtain this product? 

10. Would you be willing to participate in a follow-up conversation about your feedback?

To help us understand more about your organization so we can better tailor future products, please provide:

Name:

Organization:

Contact Number:

Position:

State:

Email:

[Privacy Act Statement](#)