Council of the European Union

Brussels, 8 May 2020
(OR. en)

7675/20
ADD 1

LIMITE

CT 24
COSI 66
CATS 27
ENFOPOL 101
TELECOM 56
CYBER 63
IXIM 48
JAI 326

NOTE

From:	EU Counter-Terrorism Coordinator
To:	Delegations
No. prev. doc.:	7675/20
Subject:	Law enforcement and judicial aspects of encryption: The various forms of encryption

The five major types of encryption usage are set out below.

1. Device encryption

Device encryption, which ensures the security of users' personal hardware, including smartphones, has reached a new level of public attention in the wake of high profile terror attacks across Europe and the US, following which law enforcement agencies have sought access to perpetrators' devices to aid in ongoing investigations and prosecutions. Europol's 2016 Internet Organised Crime Threat Assessment (IOCTA) subsequently cited the exploitation of encryption for illegal activity, on devices like smartphones, as a key impediment to detection, investigation and prosecution of serious crime.

This was reiterated in the 2019 IOCTA[1]. Apple implemented more sophisticated device encryption through iOS 8 (and all following iterations of iOS) from 17th September 2014; and since, have been at the centre of multiple legal disputes over the unlocking of their devices to **aid ongoing criminal investigations and prosecutions**[2].

Beyond these mainstream devices, the niche market for encrypted communication devices with enhanced privacy and security features specifically marketed and sold to organised crimes groups is on the rise. For example, the company Phantom Secure was recently taken down in Canada for providing encrypted devices to drug cartels[3].

The Commission addressed device encryption in its 11th Progress Report Towards an Effective and Genuine Security Union, which proposed a range of "**measures to support Member State authorities, without prohibiting, limiting or weakening encryption**"[4]. This included the pledging of EUR 5 million to Europol's European Cybercrime Centre (EC3) for development of their technical capabilities to deal with encryption, in cooperation with the Joint Research Centre (JRC).

But the capacity is still under development and has been described by Member States Law Enforcement Authorities (LEAs), as likely to be "overstretched"[5], as device encryption becomes an increasingly pressing issue. The 2019 report of the Manhattan District Attorney's office[6] on smartphone encryption shows that 64% of all devices seized by the New York Police Department are encrypted vs. 24% in 2014.

[1] See also Europol's IOCTA 2019 p. 56 : "Encryption, while recognised as an essential element of our digitized society, also facilitates significant opportunities for criminals. Investigative techniques, such as lawful interception, are becoming increasingly ineffective (or even impossible) as criminals exploit encrypted communication services, applications and devices."

[2] Of particular note is the February 2016 court case in the United States District Court for the Central District of California, in which the FBI requested lawful access to the device of Syed Rizwan Farook, one of the attackers in the December 2015 terrorist attack in San Bernardino, California which killed 14 people and left 22 injured. See also https://www.judiciary.senate.gov/imo/media/doc/12.10.2019%20Feinstein%20Statement.pdf

[3] *Second report of the observatory function on encryption*, joint report by Europol and Eurojust, February 2020

[4] COM(2017) 608 final; Communication from the Commission to the European Parliament, the European Council and the Council - Eleventh progress report towards an effective and genuine Security Union; 18.10.2017.

[5] High level stakeholder dialogue on encryption with prosecutors, DG HOME and DG JUST (13 November 2019) in The Hague

[6] Report of the Manhattan District Attorney's Office on smartphone encryption and public safety, October 2019.

2. End-to-end encryption of communications data

The encryption of communications data is not new. **End-to-end encryption (E2EE)** has been integral to the infrastructure of messenger programs like WhatsApp since April 2016. In March 2019, Mark Zuckerberg, CEO of Facebook, pledged the roll-out of a 'Privacy-Focused Vision for Social Networking' on Facebook's Messenger app through the universal implementation of E2EE on all messenger data; all the while acknowledging an inherent trade-off between privacy and security in communications data[7]. Even if these plans have not materialised yet, this shows an increasing trend of E2EE for widely used messenger programs, hence the existing problem for law enforcement will be amplified.

The impact of E2EE is that the service provider will no longer have access to the content of the communication and is therefore unable to share content in a readable form to respond to a lawful law enforcement warrant.

As reflected during the December 2019 hearing before the US Senate's Judiciary Committee[8], law enforcement and judicial authorities have not been consulted on the deployment of these encryption protocols prior to their implementation on platforms, so that solutions have not yet been found to provide responses to warrants in readable format.

The implications of widespread E2EE for lawful access are clear: severely limiting the ability of LEAs to access communications data of known/suspected criminals based on warrants, hence hampering investigations and prosecutions and increasing the risk of impunity.

[7] https://www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/

[8] Encryption and Lawful Access: Evaluating Benefits and Risks to Public Safety and Privacy, hearing before the United States' Senate Judiciary Committee on December 10th, 2019.

The proposals for E2EE would limit the ability of Facebook's own automated safety systems to detect and remove harmful content. Given that Facebook acted against 26 million pieces of terrorist content between October 2017 and March 2019[9], and automatic flagging on the platform accounts for 99% of all actions taken by Facebook against harmful content, terror-related or otherwise; the scale of the loss to user security is vast. While Facebook has so far been an active participant in the fight against terrorist content and Child Sexual Exploitation on its platform, the US National Center for Missing & Exploited Children (NCMEC) has estimated that the implementation of their 'privacy first' proposals would result in a loss of 70% of Facebook's annual reporting contributions, equivalent to 12 million reports globally[10].

After implementation, the 'privacy-first'[11] move would only allow access to unencrypted communications data if access to the user's device is gained, as with WhatsApp and many other applications currently using E2EE. When pressed on this issue in an open letter by partner countries in October 2019, Facebook subsequently published a letter in response in December 2019 which did not address the loss in lawful access to communications data[12].

With regard to Telegram, which also provides E2EE messaging services for its users, Europol's IOCTA 2019 states "… Telegram remains the platform of choice for terrorist sympathisers, who continue to exploit its advantageous encryption and file-sharing capabilities."

[9] https://transparency.facebook.com/community-standards-enforcement#terrorist-propaganda It is not clear how much of this is private content which would in the future no longer be flagged and removed.

[10] In 2018, Facebook made 16.8 million reports to the US National Center for Missing & Exploited Children (NCMEC) - more than 90% of the 18.4 million total reports that year. The UK National Crime Agency (NCA) estimates that, "last year, NCMEC reporting from Facebook will have resulted in more than 2,500 arrests by UK law enforcement and almost 3,000 children safeguarded in the UK" alone; see "Open letter from the Home Secretary - alongside US Attorney General Barr, Secretary of Homeland Security (Acting) McAleenan, and Australian Minister for Home Affairs Dutton - to Mark Zuckerberg", UK Home Office.

[11] One needs to keep in mind that in the vast majority, service providers continue to have access to lots of other user data that is then used to profile users e.g. for advertisements.

[12] See "Facebook's public response to open letter on private messaging" https://about.fb.com/wp-content/uploads/2019/12/Facebook-Response-to-Barr-Patel-Dutton-Wolf-.pdf.

3. Encryption across integrated platforms

The planned E2EE of Facebook messenger includes the additional problem of encryption across integrated platforms. As the Facebook messenger is linked to the central Facebook platform**,** criminals can **operate freely across both applications**.

Such integration gives terrorists and online predators the ability to search for and find publicly visible, vulnerable users on one open forum application; to then target and groom them using encrypted communications, or exchange harmful content, via another. Integrating encrypted applications into a platform such as Facebook therefore creates a second challenge by compounding those risks already posed by high-level communications data encryption, all the while allowing malign actors to access personal content elsewhere on the platform, which facilitates their contacting of potentially vulnerable users[13]. This is different from a WhatsApp-type situation that requires offenders to already possess the potential victim's phone number.

Losing access to the content data could also keep LEAs from spotting a potential link being sent to a dark website via Messenger. This would make the first contact or baiting of a potential victim undetectable from LEAs and would present a serious risk for terrorist radicalization and recruitment and child sexual exploitation.

4. Custom encryption applications

Custom encryption applications continue to be an issue in counter-terrorism and combatting child sexual exploitation. The ability of users to download and implement **new encryption tools tailored for criminal use** allows for higher levels of secrecy on the internet, in their communications and in the storage of their files on local devices. The *Second report of the Observatory function on encryption* by Europol and Eurojust stresses that such applications represent a "readily available" and freely downloadable alternative to costly encrypted cell phones[14].

[13] This risk was explained in detail in an open letter by the National Society for the Prevention of Cruelty to Children (NSPCC) of the UK to Mark Zuckerberg on 6th February 2020: "If Facebook Messenger and Instagram Direct are seamlessly integrated into large open platforms, abusers will be able to exploit existing design aspects to make easy and frictionless contact with large numbers of children, and then rapidly progress to sending end-to-end encrypted messages. This presents an unacceptable risk to children".

[14] *Second report of the observatory function on encryption*, joint report by Europol and Eurojust, February 2020, p.19

Custom encryption apps are often easily accessible in the AppStore or the Android marketplace. Some of them are free, others such as SkyECC or Encrochat have to be paid.

Examples of custom encryption apps include 'Mujahedeen Secrets', an open-source encryption program for Microsoft Windows, released by Al-Qaeda's media arm, Global Islamic Media Front, in 2007, to be used by jihadists to protect the confidentiality of their electronic messages.

Custom encryption applications can be a significant challenge for investigators. High profile criminal networks have the resources to hire top level experts. It takes significant time, investments and resources for LEAs in research, reverse engineering, etc. to get lawful access to relevant information in the context of an investigation. The significant and ever increasing resources and investments required by LEAs to tackle custom encryption applications risks **creating safe havens for criminals to communicate and exchange content** related to terrorism and child sexual exploitation.

5. Encryption of internet protocols

The issue of encryption of internet protocols is complex, multi-faceted and requires further analysis, including of related issues.

Encryption of the protocols underpinning the basic functioning of the internet include privacy-centric services rolled out by Internet Service Providers (ISPs) and browser makers are designed to render previously unencrypted, and therefore potentially lawfully accessible, internet traffic data encrypted.

This encryption of the communication between users (and the queries they make) and websites they are trying to access makes **existing lawful law enforcement access to internet traffic or search metadata** of criminals based on a warrant much more difficult.

Of particular note is the widespread rollout of the DNS-over-HTTPS (DoH) protocol for internet traffic[15]. This protocol has already been trialled by Mozilla on their Firefox browser in the US, with the intention of rolling it out as standard in other parts of the world over the coming years[16]. Google has also trialled the protocol on Chrome[17]. In November 2019, Microsoft announced that they intend to transfer to this new DoH protocol[18]. This indicates that, without intervention from national governments based on law enforcement needs, this encrypted DoH protocol is to become a market standard for browser makers in the coming years.

DoH makes law enforcement access more difficult, but in and of itself does not preclude law enforcement in principle from accessing related, non-encrypted traffic data. However, this might change in the future given the trend to encrypt more and more. Access is still possible through the cooperation of ISPs on the DNS queries of the users provided that these queries are resolved locally, using DoH enabled resolvers lying under national jurisdiction.

[15] The DNS-over-HTTPS protocol takes the Domain Name System (linking domain names, as part of website URLs, to IP addresses i.e. "resolving" the Domaine Name System) and encrypts it using the secure extension of the HTTP (HTTPS), the request-response protocol connecting clients with the servers they're trying to access online. DNS requests are usually publicly visible in internet traffic, and therefore could be lawfully accessed by law enforcement authorities. The DoH protocol securely encrypts this process and prevents the linkage between domain names and IPs, making it much more difficult to link harmful domains, and their content, to IP addresses. DoH also makes networks more secure, by making it more difficult to commit man-in-the-middle (MITM) attacks. DoH is just one of several trialled encryption protocols, including the DoT (DNS-over-TLS) protocol, but DoH has come to dominate the space.

[16] https://support.mozilla.org/en-US/kb/firefox-dns-over-https

[17] While Google has trialled the DoH protocol, they have also pledged to respect national DNS resolution by continuing to use a local DoH enabled resolver as the default and so the resolving (i.e. matching site URLs with server IP addresses) could be provided locally by the ISP under national jurisdiction. This would leave DNS resolution within national jurisdiction and hence allow for lawful access of national law enforcement. Mozilla's Firefox browser will instead provide DNS resolution by Cloudflare, which is US based, as a default setting, adding an additional cross-border element. Cloudflare will only store data in its distributed 'edge' network for a maximum of 24 hours prior to permanent deletion.

[18] https://techcommunity.microsoft.com/t5/networking-blog/windows-will-improve-user-privacy-with-dns-over-https/ba-p/1014229

It seems that the encryption problem might be linked to an e-evidence problem: The risk for national law enforcement lies in the combination between this encryption of the DNS query and the use of a "remote" resolver, provided by the browser for example. Until now, queries were directed to resolvers offered by the national ISPs (ISPs see it as their responsibility to offer DNS resolution, although there is no regulatory or contractual basis for this and users are free to choose another DNS resolver). But in the future, some browsers, such as Mozilla, offer to use their US based resolver as the default resolver for the DNS queries of their users. The resolving then lies under US jurisdiction and access to it by national law enforcement has a cross border impact. It might still be possible for the user to change the default setting to rather use a local resolver. However, most users don't proactively choose their DNS resolver, so that de facto the international browser makers dominate the resolver market, making the reach of local law enforcement much more difficult.

In addition, depending on the method of deployment[19], this new encryption protocol might no longer enable implementation of national laws to prevent access by end users to certain identified harmful content such as child sexual abuse material or other content endangering safety and public order. Currently, most of the filtering concerning requests is carried out by Internet service providers at the DNS resolution level. With the DoH protocol and a US based DNS resolving, those filtering requirements would only be applied by browsers to the type of content for which US authorities require filtering and the local ISPs would no longer be able to implement national requirements on filtering. Similarly, other existing solutions provided to protect citizens online might also be hindered: A large German Internet service provider for example has developed an end-to-end solution to takedown or disable large botnets. This kind of solution depends heavily on the ability of ISPs to evaluate DNS queries and responses.

[19] This risk is only present if DoH is deployed in the way described in the preceding paragraph. Several browser providers (Google, Microsoft) are planning to enable DoH in Europe exclusively if the relevant local ISP offers an in-house DoH resolving service. Hence, it seems that in this scenario ISPs in the EU will be able to continue the implementation of national laws and filtering activities.

Beyond the rolling out of DoH, which still preserves some capacity to access data, the accessibility of internet traffic data more globally may be at risk as the Internet Engineering Task Force (IETF), which develops and promotes internet standards, has indicated that it intends to promote the roll-out of encryption of other protocols composing the architecture of the internet, which together may prevent lawful interception of criminal's internet traffic, thereby starving LEAs of information necessary for their online investigations. The absence of representation of LEAs and governments in general in the standard setting bodies (such as Internet Engineering Taskforce) leads to insufficient inclusion of their priorities in the creation of internet standards. The Commission has pointed out the risk that "browsers could potentially dictate unilaterally the requirements for DNS resolving"[20]. Furthermore, the DoH protocol might be deployed in the future beyond browsers in various applications and in Internet of Things (IoT) devices as well.

---

[20] See Commission working paper 1939/2020 INIT "Deployment of DNS-over-HTTPS - Background paper from the Commission" used at informing the discussions of the 18 February 2020 TELECOM Working Party