

# The EARN IT<sup>1</sup> Act of 2020

## and its implications for encryption and EU decision making

### Introduction

- ) The EARN IT Act of 2020 is a **proposed US legislation** aiming to amend the Communications Decency Act of 1996 (CDA), and in particular the **section 230** by adding special protections for the **prevention** of **Online Child Sexual Abuse Material (CSAM)**.
- ) Timeline (steps: Senate-House-President-Law):
  - ) 5/3/2020: Introduction of first text in US Senate, with the Bill [S3398](#).
  - ) 20/7/2020: Unanimously (both parties) the US Senate passed the Bill, after **an important amendment on encryption**, see [here](#) the amendment. More on this later.
  - ) 2/10/2020: The Bill was introduced to the House.
  - ) Next steps: not known yet.
- ) Main elements of the Bill:
  1. to create a **National Commission** On Online Child Sexual Exploitation Prevention, a 19-member panel. The Commission once formed will **develop and continually update a Best Practices document aimed to provide guidance to service providers to help them to prevent child exploitation and aid in investigation of such crimes.**
  2. to **add** to Section [230](#) the following provisions:
    - allow any US state to bring a lawsuit to service providers if they fail to deal with child sexual abuse material on their service. For many this provision means the end of the good times for ESPs in USA and consequently for the internet as we know it, that existed since 1996 thanks to the full immunity<sup>2</sup> of ESPs against illegal content that was in place with the section 230.
    - [This was the amendment that was done in order to face the strong criticism regarding encryption!] a service provider is not violating the law only because (i) utilizes **full end-to-end encrypted** messaging services, device encryption, or other encryption services, (ii) **does not possess the information necessary to decrypt a communication**, and (iii) **fails to take an action that would otherwise undermine the ability of the provider to offer full end-to-end encrypted**

---

<sup>1</sup> Eliminating Abusive and Rampant Neglect of Interactive Technologies

<sup>2</sup> Section 230 had given since 1996 to the Electronic Service Providers (ESP) the following important privileges: (i) full immunity, regarding the content that is posted or exchanged through their platforms, and (ii) the right (voluntarily) to screen, filter and remove user content that THEY consider to be “obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable.”

**messaging services, device encryption, or other encryption services.**

- ) The [opponents](#) of the EARN IT say that there will be a negative impact for the freedom of speech, the freedom of expression, and that the existing small ESPs as well as the new entrants will not be able to survive because of the liabilities that will have to carry in order to avoid legal persecution in the future.
- ) The supporters of the EARN IT Bill on the other hand say that the EARN IT will be the beginning to solve problems related to the powers of tech giants, also in the political debates and to solve issues related to the facilitation of CSAM, hate speech and ideological biases.
- ) [Lindsay Graham](#), the author of the EARN IT Bill asserted that social media companies and internet service providers would be able to defend themselves in a civil suit as long as they employ "the best business practices." that will be produced by the competent committee that would be established by the Act. This means that these 'best practices' will be **compulsory technologies** for ESPs to avoid persecution.
- ) It is not the first time that the section 230 is amended. In 2018, Section 230 was amended by the Stop Enabling Sex Traffickers Act (FOSTA-SESTA) to require the **removal of material** (not the prevention) violating federal and state sex trafficking laws. But this cannot be compared with the EARN IT Bill as the latter brings clear and strict rules and liabilities for ESPs, while the former has been criticized for its 'loose' enforcement.

## **Implications of the Bill for encryption**

- ) After the amendment on encryption, the Bill **does not preclude end to end encryption, nor asks the ESPs to provide the encryption keys, nor asks for weak encryption**. In other words, full end to end encryption as well as strong encryption in general is possible. But this does not mean that the ESPs will not implement CSAM prevention measures.
- ) Security specialists and IT engineers say that the obvious way to prevent CSAM in the presence of strong and e2ee is to **screen information before and after is encrypted**.
- ) According to [this](#) article, 'Encryption Continues to Be a Live Issue' **as in case the ESPs utilize strong encryption or e2ee** they will have to face difficult technological challenges in order to ensure the prevention of CSAM by utilizing 'best practices' proposed by the competent committee. The article also suggests these 'best practices' will take the form of **compulsory technologies** and might include things like **client-side scanning**, where the system takes a "fingerprint" (also called a hash) of each of a user's images and videos before they are sent as messages, to compare against a database of known CSAM. If the hash matches something in the CSAM database, the system prevents the message from being sent (and could also report that message to some authority). Theoretically, a system that uses client-side scanning could still send messages encrypted end to end, with **backdoored e2ee technologies**, i.e. screening of information before or after actual encryption.

- ]
- the CSAM data bases are too large to be stored on user devices like smartphones, even in compressed form. Also in case they are stored in the device, these databases would become available to malicious actors and most probably they would facilitate the manipulation of the detecting technology. This means that the only realistic option is to have the **CSAM databases and the hash comparison outside the device**, possible in the ESP or in another trusted party. Further analysis is needed as how sensitive these hashes are and how the hashes of user's content can be protected outside of the device.
  - the primary algorithm used for scanning images and videos is PhotoDNA, which has not been publicly released (raising a whole other set of abuse concerns), most likely because it is **fragile, and thus susceptible to bad actors reverse engineering and circumventing it**. Thus, it is likely not possible to deploy PhotoDNA on consumer devices without risking that it will become ineffective everywhere it is deployed, or creating a slew of additional security concerns.
- ]
- From the above problems, we understand that despite the encryption amendment, **the structure of the EARN IT act is intrinsically antithetical to a robust e2ee ecosystem**. Companies will be **disincentivized from building and maintaining e2ee systems** out of fear of lawsuits, and will still likely be forced to handle their users' messages in ways those users would consider a violation of trust and confidentiality.


## Implications for EU decision making (if the Bill becomes Law)

- ]
- After [December 21 2020](#), **electronic communications USA ESPs providing services to EU citizens will automatically fail to comply with the ePrivacy<sup>3</sup> Directive**. This is the reason that many USA ESPs [oppose](#) EARN IT, and even [threaten](#) that they will leave US soil if EARN IT becomes law.
- ]
- Also, in general USA ESPs providing services to EU citizens will face challenges against **GDPR compliance**, as a result of the EARN IT extra moderation-screening (with or without encryption) of content of their services in order to prevent CSAM. This is relevant to the recent EDPS Opinion 7/2020<sup>4</sup>, where we see the problems with compliance against GDPR if such practices are applied.
- ]
- The 'indirect' circumvention of encryption for US ESPs, will also automatically put the requirements of the **SCHREMS II judgement** in question.

---

<sup>3</sup> On 21 December 2020, with the entry into application of the European Electronic Communications Code ("EECC"), the definition of electronic communications services will be replaced by a new definition, which includes number-independent interpersonal communications services. From that date on, these services will, therefore, be covered by the ePrivacy Directive, which relies on the definition of the EECC. This change concerns communications services like webmail messaging services (signal, wire, whatsapp, messenger, imessage, etc) and internet telephony.

<sup>4</sup> on the Proposal for temporary derogations from Directive 2002/58/EC for the purpose of combatting child sexual abuse online

- 
- ) At the same time, **EU ESPs will not be able to provide services to USA customers**, as they will face EARN IT requirements and will risk being legally persecuted.
  - ) [Both](#) Trump and Biden were in favor of EARN IT act, and in general they are in favor of more restrictions and control of ESPs, especially the tech giants. This means that **the political momentum is in favor of EARN IT**.
  - ) Also the **COVID19 worldwide situation is in favor of EARN IT**, as [many](#) support that CSAM has exploded during COVID19 together with other illegal activities in the midst of the general explosion of digitalization.
  - ) The impact of EARN IT on the [EU digital services act](#) needs to be analyzed. It's worth mentioning that the EU Parliament, has conducted a relevant to EARN IT [study](#) in June 2020, named “**Online Platforms' Moderation of Illegal Content Online**” in order to review and assess the EU regulatory framework on content moderation and the practices by key online platforms. On that basis, it makes recommendations to improve the EU legal framework within the context of the forthcoming Digital Services Act.
  - ) At a political level EU will be seen by USA government as actually not taking measures to **prevent the propagation of CSAM material for the sake of privacy and data protection**.
  - ) There is a ‘paradox’ that will need to be solved: until December 21, electronic communications services ESPs based on both USA and EU are free (on a voluntary basis) to support the detection/prevention of CSAM using screening and moderation technologies like photoDNA, while (i) after December 21 this will not be possible for EU ESPs thanks to the application of ePrivacy, and (ii) after EARN IT becomes law this will be mandatory for USA ESPs, according to specific compulsory technologies (including probably photoDNA).