European Parliament

30.04.2020, Brussels

Open Letter to the U.S. Senate concerning the EARN IT Act

Honorable Representatives of the United States Senate,

we, the undersigned Members of the European Parliament, support the long-standing partnership and cooperation between the European Union and the United States of America in the spirit of our shared core values of liberty and freedom.

Our present is marked by the rise of digital authoritarianism and ubiquitous mass-surveillance by hostile state actors and private and corporate entities alike. We are witnessing the 14th consecutive year of deterioration in global freedom. Privacy and security in the digital realm are a luxury good that not many in the world can afford and it is getting harder to get by. Private, secure communication is a foundation for free speech and a free democratic society. If citizens are deprived of the ability to speak and interact freely with one another with the presumption of innocence and without fear of state prosecution, democratic checks and balances cannot function. We believe that the European Union and the United States must join together to preserve and promote secure and uncensored free speech and to offer the world a moral, legislative and commercial alternative to digital authoritarianism.

The U.S. Constitution enshrines the protection of free speech in its first amendment. Likewise, the fourth amendment protects US citizens against unreasonable searches and seizure by the government, and thus against arbitrary government surveillance. A wealth of Supreme Court decisions has clarified and developed the scope and circumstances under which these rights apply to modern, digital, user-generated communication.

The EARN IT Acts' (S. 3398) goal is to prevent the online sexual exploitation of children. The currently considered Act will likely not achieve much on this imperative objective; instead it will have calamitous consequences for free speech far beyond the United States. We are concerned that this bill would directly affect how U.S. companies gather and process data from European customers, as well as how European and other companies would have to provide their services to American citizens. In its current form the act would likely violate the first and fourth amendment of the Constitution and would create the competitive necessity for good-faith online service providers to initiate mass censorship, surveillance and to create backdoors to their users encrypted communication.

The Act would not exclusively target unlawful child sexual abuse material (CSAM); instead it sets out to regulate how online service providers should control user-generated content in general. Providers would be forced to engage in editorial activity or risk losing legal immunity for user-generated content under Section 230 of the Communications Decency Act. The plan to make online service providers earn Section 230 immunity by complying with recommended best practices is threatening its whole purpose as it will have almost no effect on the majority of bad

actors. Providers of malicious content, based mostly in the dark web, already don´t qualify for Section 230 immunity, as they are directly involved in the illegal content on their sites.

Instead, commercial entities will have to choose to engage in censorship of inconceivable volumes of data, which would only be achievable via automated filters and pattern recognition software with all its biases, errors and shortcomings or risk losing legal protection.

End-to-end encryption is fundamental to the safety, security, and privacy of speech worldwide. Requiring backdoors to encrypted services as a necessary new best practice would force online service providers to either break their value proposition to their millions of customers by effectively giving up encryption or force service operators to abandon the United States' market and move operations elsewhere. Online service providers are already legally required to report any CSAM that they have knowledge of. Persons engaged in illegal commercial activity with CSAM will not be stopped by the breach of encryption services on popular platforms and will continue to encrypt their illegal content prior to using commercial online services. The systematic and disproportionate surveillance and censorship of commercial online service providers would thus likely not result in a drop in CSAM.

Applications with end-to-end encryption are routinely used by both EU and U.S. government officials and are required and recommended by the United States military and intelligence as well as European Governments and the European Institutions. We appeal to you to ensure the protection of free, secure speech and privacy in the digital domain in your efforts to prevent online sexual exploitation of children.

Respectfully,

MEP Markéta Gregorová

MEP Alviina Alametsa
MEP Konstantinos Arvanitis
MEP Margrete Auken
MEP Patrick Breyer
MEP Gianna Gancia
MEP Francisco Guerreiro
MEP Marcel Kolaja
MEP Karen Melchior
MEP Niklas Nienass
MEP Mikulas Peksa
MEP Kira Peter-Hansen
MEP Salima Yenbou