

Intermediary **Liability** Blog

The Evidence Hub for Policymakers

Illegal Content: Safe Harbours, Safe Families

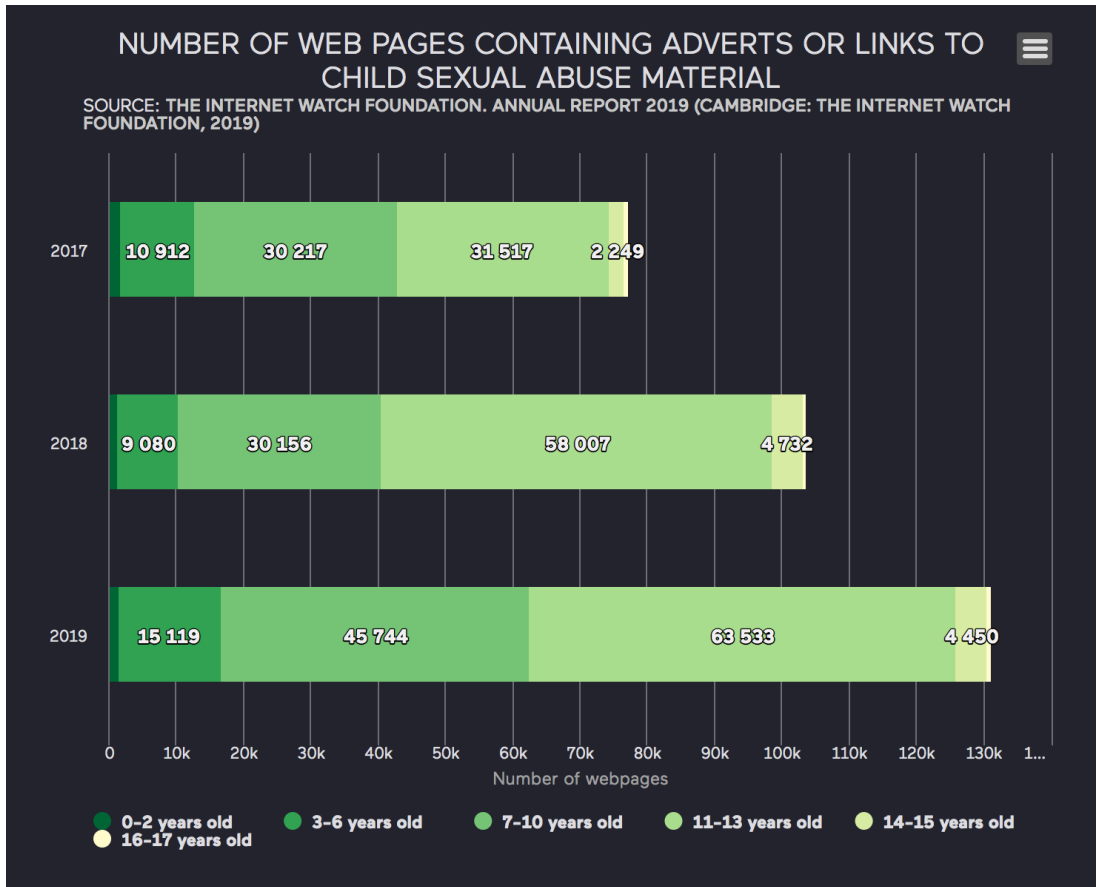
28 May 2020 | Estimated reading time: 4 minutes

The rules on illegal content are clear: if it's illegal in the real world then it's illegal online. Platforms and regulators have seldom sparred over this; the community guidelines enforced by most platforms are straight-forward. Content suspected of being illegal can be flagged for inspection – or blocked at upload – and should be removed as quickly as possible if it turns out to be unlawful. This zero-tolerance rule applies to many types of illegal material, but it applies first and foremost to child pornography and images of children being abused.

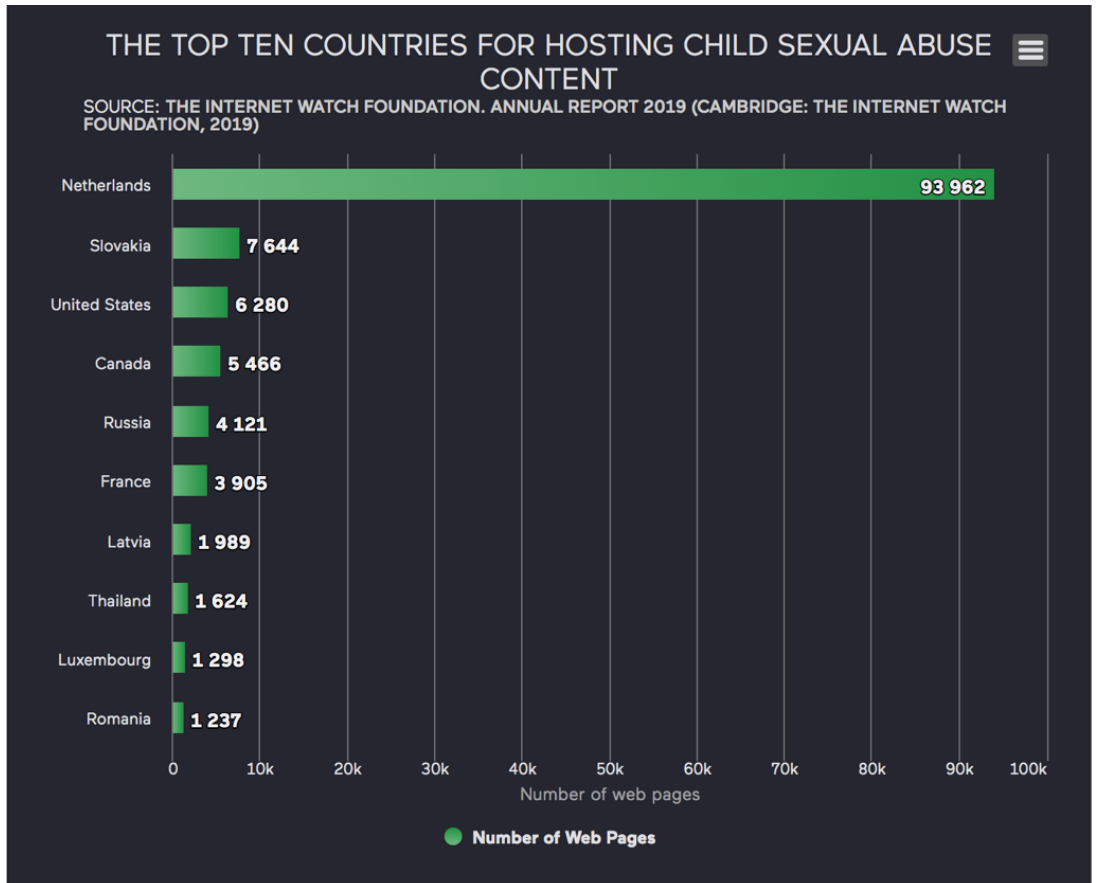
Many platforms have invested heavily in artificial-intelligence to help them spot and block illegal content before it even goes up – so much so that some images, like the iconic picture of a naked Vietnamese child running to escape an American napalm attack, have been incorrectly flagged and temporarily barred (a subsequent human review saw the content restored and the algorithms tweaked).

The questions become trickier when legal liability is brought into the picture. In 1996, the United States set the rules that would become the standard; according to [section 230 of the communications decency act](#), platforms would be expected to “use good faith” to restrict access to content that was “obscene, lewd, lascivious, filthy, excessively violent, harassing or otherwise objectionable” and would enjoy legal immunity from prosecution over content that users posted (including prosecution for removing user-posted content that fell foul of the platform's community guidelines). In Europe, article 14 of the [electronic commerce directive](#) (2000) did the same; it said platforms were not liable for content posted on their site if they had no prior knowledge of the illegal nature and if the platform acted expeditiously to remove it once notified.

The disturbing thing is the amount of child-abuse material available online is rising. The volume of content hosted on websites containing sexually abusive material has increased a staggering 70% since 2017, according to an [Internet Watch Foundation report](#).



To be clear, the platforms themselves are not guilty of this rise; much of the material appears on stand-alone websites. Shockingly, 90% of those websites originate in Europe.



No one supports the use of the Internet to aid and abet crimes against children. But the question of whether the rules are tough enough – and whether platforms are doing enough – is in clear dispute. But so is the flip side of the argument: platforms use filters to flag and remove content; have these become too sensitive? Is the law inching towards censorship and surveillance? Do lawmakers need stronger tools for tracking criminal activity online? Or is there an emerging threat to privacy slipping in under the banner of stopping crimes we all know and feel to be horrific?

And perhaps more pointedly, is the horrendous fact of the continued existence and spread of online child pornography – and the evident need to respond with strengthened measures – being used as a convenient screen for compelling platforms to allow political parties – some led by powerful politicians – to spread lies without being challenged?

In May 2020, U.S. President Donald Trump [announced a formal “review” of the section 230 exemption](#), charging the platforms with political bias after one platform posted a link to correct information next to a tweet containing proven and provable lies. Earlier, U.S. Senator Lindsey Graham, a South Carolina Republican, introduced a sweeping bill on [Eliminating Abusive and Rampant Neglect of Interactive Technologies \(EARN IT\) Act](#) that would allow the platform liability exemption to be lifted in certain cases. Under the proposed rules, a 19-person committee would elaborate a code-of-conduct on content-removal (which the U.S. Attorney General and the U.S. Congress would ratify and amend); companies that failed to meet the tough standard could see their legal immunity from prosecution lifted, opening the door to lawsuits from aggrieved parties who felt that harm had been generated or their rights abused by material circulated on the platforms.

Law enforcement officials – including U.S. Senators sponsoring the bill – say the platforms still don’t do enough to stop illegal content from spreading; with the support of several Democratic Senators, they seem to be carving out a middle ground where platforms could keep much of their legal immunity but where, crucially, guidelines approved by the U.S. Attorney General (currently a controversial Republican) could be used to lift or suspend it in some cases.

Privacy advocates see additional threats; they say the law could be used to force companies to open backdoors on end-to-end encryption, an increasingly popular way of communicating and exchanging information. Or it might possibly lead to pre-emptive curbs on the use of end-to-end encryption itself.

The European Commission has also promised new rules “for a more effective fight against child sexual abuse” later this year, according to the [2020 work programme put forward by President Ursula von der Leyen](#). And the U.S. law’s final contour isn’t known. To be sure, [class action suits are how the U.S. established high product safety standards](#) in areas as diverse as automobiles, children’s toys, lawnmowers and airplanes. But the risk is the power the proposed law would give political figures to lift immunity and allow lawsuits against platforms which challenge their authority on the most basic points of truth and evidence. Recent history has shown that U.S. administrations – and this one in particular – are not always impartial and don’t shy away from using the tools of state for political ends.

Which leaves the horrific problem of child abuse online. Whatever the modalities, regulators should set aside their potentially harmful games and work with industry and privacy advocates to curb this scourge that no one wants and everyone would like to see end. Its rise is a shame and a disgrace that should concern us all. But attitude and scorn are not sufficient tools for fighting it. And political witch hunts will be very distracting and even less effective. The best response would be to take the issue seriously, craft joint responses and tackle the problem collectively. That's what voters want. That's what society needs.

PAUL HOFHEINZ

Paul Hofheinz is president of the Lisbon Council.

This blog post appeared on the Intermediary Liability Evidence Hub, an interactive website managed by [The Lisbon Council](#), a Brussels-based think tank, to gather available evidence and data points on the issue of intermediary liability. Its website is <https://evidencehub.net/>.