Summary Report of Grassroots for Europe Round Table #39:

The Online Safety Bill and why you need to know about it.

Tuesday September 5th, 2023.

Session theme and context

We were delighted to be joined in this session by an expert chair and panel to focus on the Online Safety Bill, a large, complex and dangerous piece of UK government legislation nearing the final stages of its passage through Parliament. The Bill has been widely and credibly seen as a major threat to democratic and European rights and freedoms. At the same time, similar measures have been proposed in the EU, some of which raise similar concerns.

Chair's introductory comments

Dr Monica Horten (independent policy advisor): Our topic today is the Online Safety Bill and one specific issue raised by this monstrously vast and multifarious piece of legislation, which is absolutely unacceptable. That is what we can call the WhatsApp issue: the Bill's requirement that technology platforms for internet communications and services proactively monitor and exclude forms of content – such as content related to terrorism and child sexual abuse - which are either illegal or deemed 'legal but harmful'. This part of the Bill, which has had some recent media exposure, has caused Whatsapp (among other providers) to say that it will take its services out of the UK, because it believes it will no longer be able to operate those services and keep people safe at the same time. The problem is that the measures that the government wants will force WhatsApp and other providers to compromise their encrypted messages in order to conduct mass surveillance of people's everyday personal and business communications. The Bill is like other controversial recent pieces of UK legislation which don't define things

properly and create dangerously open-ended ministerial and regulatory powers. It gives itself lots of wriggle room and lots of wriggle room for the police and others to interpret the law. It creates a skeleton law which thinks others can fill in later on. These things all create problems and new risks of harm. And the measures that the government wants to include will not necessarily achieve the policy aims that it says it wants to achieve. We are pleased to have with us three domain experts to take us through key aspects of the issue as well as concurrent developments in the European Union.

Robin Wilton [The Internet Society]

Robin has worked in IT since the mid-eighties, having been tech. support for IBM's Europe, Middle East and Africa banking and hardware encryption products. Until the late 1990s these products were regulated in the same way as munitions, with encryption allowed only by banks or government bodies. Encryption was strictly limited by length of key – this determining how difficult it is to decrypt messages. However, although this has always been an area where governments have tried to regulate, towards the end of the 1990s this was no longer viable because current economics, with on-line commerce, meant everyone needed secure communication. Now we all rely on encrypted communications and other aspects of encryption which make authentication work when we log in. Without encryption, all on-line activities become subject to attack. To quote Paul Nemitz (Principal Advisor, European Commission Directorate-General for Justice and Consumers) with whom Robin recently moderated a panel, "If citizens can't have private conversations, you can't have a functioning democracy."

If you search online for Online Safety Bill, one likely "hit" will be to the Government's own "guide to the Online Safety bill", which says that the bill "*will make social media companies more responsible for their users' safety on their platforms".* Although most people can name about half a dozen social media companies, this bill will actually affect some 25,000 UK companies, all of which could potentially be criminally liable if they do not comply with the requirements of the Act. However, the government fails to specify "safe" from whom or from what. By constraining fundamental rights, such as freedom of expression, access to information and freedom of assembly, the bill may do more harm than good. Justification for the bill is primarily expressed in terms of terrorism and child sexual abuse. But the measures it proposes to protect users from these evils also expose them to other forms of

malice and attack. In weakening the security of online products and services the government is putting more people at risk, including the very children and vulnerable individuals it claims to protect. In the face of evidence, it is clear that the government is not, overall, motivated primarily by the safety of children.

The Online Safety Bill mentions encryption only in the context of saying that if an organisation is served with a warrant or request for information as to how users are protected and that information is encrypted when submitted, this constitutes an offence.

It threatens to make it impossible to have an encrypted conversation but doesn't mention encryption in any meaningful sense. How and why was this achieved? In the past the government simply regulated the length of keys used for encryption – the longer the key the harder it is to break the encryption. For example, the encryption security of a home Wi Fi has options called WEP, WPA and so on. These vary in the length of key they use, the smallest keys being 40 bits long and easy to break. Until the late 90's government regulation as to the length of keys allowed in commercial software worked. However, the development and publication of encryption algorithms meant that regulation through control of keys was no longer viable. So, government started to require backdoors or front doors, either through weakness in algorithms or so-called key escrow. Key escrow is like getting a locksmith to fit new locks to your front door; you are handed two keys and a third one is lodged with the police should they need access to your house "for your safety and convenience". Key escrow can be made to work in software just as in hardware keys, but it can't be made safe. The more keys there are, the more people can gain access to those keys. It's easy to imagine how those responsible for a government repository for keys, could be open to blackmail, extortion or physical attack.

Since key lengths, encryption backdoors, key escrow cannot be used safely in a modern digital society (in fact, they break the very things we rely on to keep us safe) - the government has taken a different approach. It does not mention encryption at all, merely saying that an organisation is liable if it allows illegal material to be distributed or communicated via the service it offers. It makes the service provider liable for the behaviour of its users, a bit like making a car manufacturer liable if people drive their cars badly. In these circumstances, the car manufacturer might impose severe restrictions. Similar reaction would likely come from service providers for use of their products and services. The response from WhatsApp appeared to be that this would make it impossible

to offer the service in the UK. However, Meredith Whittaker – president of the Signal Foundation – says this has been misinterpreted. What she actually said was that it would be impossible for Signal to offer their product in the UK with its current level of security. If this bill is enacted, it is likely that Signal will continue to offer its product in the UK until the Government forces it to withdraw – putting the onus on the Government to demonstrate its opposition to confidentiality.

Essentially, the bill allows the government - via its enforcer, Ofcom - to go to any company, WhatsApp, Signal, BT, Virgin or indeed any online search engine, and say that company must take appropriate technical steps to detect whether users are communicating or sharing illegal material – encrypted or not. If the company fails to comply, government will compel the company to accept technology from outside to be bolted on to its systems thus giving access to encrypted content to law enforcement agencies. This raises important questions as to the source of the bolt-on technology, - what does it do, who approves it, how certain is it that it works and how accurately? By and large the bill does not address these questions, talking merely of accredited technology, meaning accredited by Ofcom or another person appointed by Ofcom – which one can assume is code for GCHQ. Accreditation is defined as meeting “minimum standards of accuracy in the detection of terrorism content or child sexual exploitation and abuse content”. But then, what constitutes these minimum standards of accuracy? For the time being, minimum standards are defined as “those approved and published by the Secretary of State following advice from Ofcom”.

So, the Online Safety Bill is chasing its own tail, getting advice from someone we don’t know, to accredit something we can’t see, but which we are assured will do what we’re told it will. There are certainly serious issues in the way in which this bill has been written.

Ella Jacobowska [EDRi – European Digital Rights]

Both the EU Digital Services Act (DSA) and the Child Sexual Abuse Regulation have areas of overlap with the UK Online Safety Bill. The DSA - the EU’s recently adopted attempt to deal with illegal content online – came into force at the end of August (2023). However, whereas in the UK much of the discourse focuses on “harmful” content, which is not actually illegal, the EU’s focus is on removing illegal content such as terrorist content or hate speech. Whilst there are strong grounds for removing illegal content, it is far harder to

define harmful content. Questions arise as to who finds it harmful, do we have the right to post it, what happens to this content? This approach underpins the work done by European Digital Rights (ESRi) which focuses on the toxic business models of big tech companies and their attempts to get people to spend as much time as possible on their platforms. Outrage, emotive issues and harmful – sometimes illegal – content can be beneficial to big tech. It was hoped that the DSA would not be limited to merely looking at content moderation and rules for removing illegal content but would consider how companies profit from manipulating users and would investigate the structural core of why we have so much harmful and illegal content. Although there are some positive aspects to the DSA, its statement that general monitoring is illegal in the EU may be considered disappointing. Specifically, the DSA restates that both general monitoring and constant scanning of people's communications, even if these are public, are illegal, albeit with some extremely narrow exceptions. This is where the EU and UK approaches diverge. According to EU law, companies are liable only if they know that there is illegal content on their platforms and they cannot be held liable for everything users do.

The EU has decided to define companies subject to its rules as "very large online platforms". However, the DSA is already proving to be very contentious. Since its application, an online retailer of clothes, shoes, cosmetics, etc. has gone to the Court of Justice arguing that the rules should not apply to them as they host adverts. At ESRi, we consider what is feasible and appropriate in a democratic society and aim to prevent big tech companies from becoming sole arbiters of our online speech. So, whilst there are positive aspects to the law – no general monitoring, no mass surveillance – it fails to rein in business models. It will rely on enforceability, an area in which the EU's track record does not give grounds for great optimism.

Child sexual abuse regulation (CSA) is a new law, proposed in 2022, still being negotiated by different EU institutions, and not yet enforced. Resistance emanating from some of these institutions gives rise to some optimism that democracy and the rule of law are not dead. The law was drafted by Home Affairs with the purpose of complementing the DSA, which by not covering private chats such as WhatsApp, Signal, Reddit or emails, will fail to effectively combat child sexual abuse. However, the CSA regulation completely undermines the prohibition of general monitoring by saying that everyone is suspect until proven innocent and that their communication can be scanned. The notion of "chat control" emanated from the European Parliament with the meaning that all personal

messages could be scanned, monitored and reported to big tech platforms. These big tech companies would then have the legal obligation to report to the police who, in some EU states, are required to investigate. This would apply even if there were a 99% probability that that a parent took a photo of their child in the bath or at the beach or if the photo was of consenting young adults. Clearly, there would be potential for catastrophic outcomes with the concept of “innocent until proven guilty” being turned on its head. In the offline world policing in a democratic society starts with a justifiable suspicion of wrong-doing, which only then can lead to the issuing of search warrants. The proposal to start by casting a wide net would generate vast numbers of false alerts, potentially causing serious harm to innocent people, and goes to the core of our human rights.

EDRi have also focused on other aspects of the EU’s proposal. For example, mandatory age verification for access to certain services may sound acceptable, but it would mean that everyone had to provide an ID document or use eID to access every message service and probably other services too. This risks the exclusion of those who do not have the correct form of ID or are not sufficiently tech-savvy. If someone knows that their ID document is linked to their entire internet history, even to things which they are fully entitled to search for, they may be unwilling to provide this ID. There is a similar issue with encryption here as in the UK legislation, in that the EU text doesn’t even mention encryption. There is, however, an accompanying 400-page Impact Assessment which considers all the details of encryption and ultimately admits that there is no way to scan encrypted messages without infringing human rights. Nevertheless, in the face of advice from some 500 scientists and cyber-security experts from around the world, the Commissioner in charge has gone on the record several times claiming that such tools do in fact exist. The EU approach has been characterised by aggressivity and the implication that anyone opposing its proposal does not care about children. Consequently, some members of the European Parliament feel they have been subjected to moral blackmail.

However, unlike in the UK, the criticism levelled at this EU proposal is unprecedented, with stakeholders saying that the Commission has got something terribly wrong. These stakeholders include independent lawyers, lawyers advising EU countries, child rights and child protection groups, civil society groups, technologists, police forces, prosecutors and the UN Commissioner for Human Rights. Eight, possibly ten, EU member states are currently raising urgent concerns about mass surveillance. At EDRi we are applying every available pressure to enforce a rethink as the false dichotomy of privacy versus children

does not serve anyone. Claims of technological neutrality by both UK and EU legislators are in reality technical naivety.

In the EU tech companies, who are allowed to make their own choice of tech, have raised their concerns but not threatened to withdraw their services. In the UK the regulator, Ofcom, will choose the tech without oversight. As far as the EU proposal is concerned, there is every intention for its powers to be very widely applied, but there is some hope that the UK Online Safety Bill will not use this kind of scanning. In conclusion, opposition, both in the EU and the UK, amounts to a common fight to protect not just privacy and free expression online but all the human rights to which our online activities give us access.

Jen Persson, [‘Defend Digital Me’]: The Online Safety Bill - Children’s Rights or Child Protection?

Defend Digital Me’ (defenddigitalme.org) focuses primarily on privacy and related data ‘ 'rights of children, mainly in the education sector. The technology and policy in the Online Safety Bill relates closely to our publication with the Child Rights International Network in (January 2023 (Privacy and Protection: A children’s rights approach to encryption — CRIN

The debate about children's rights and use of online technology is often mistakenly framed as a divide between child protection and civil liberties. This allows little scope for **simultaneous** debate about children’s rights and privacy and child protection. The Online Safety Bill is not fundamentally about child sexual abuse or access to pornography, it is basically about access to content online. The Conservatives aimed in 2010 to make the internet less commercialised for children, but that focus shifted to child safety and the notion of “legal but harmful” online content with special reference to children. The tag “legal but harmful” is troubling in its all-encompassing vagueness, especially because it will be defined by undetermined third parties, is poorly drafted in the bill, and undermines the rule of law. In work that we did together with Child Rights International Network we heard heart-rending experiences of working in children’s rights, child sexual abuse, and child ‘safety’ and it comes to dominate debate which is understandable. But the question of who defines “safe” is deeply troubling. The OSB defines equally vaguely the “proactive or accredited technology” which will be granted “permitted access” to private communications to spot illegal or “legal but safe” content. The vagueness will obscure transparency. The OSB may not talk about breaking encryption, but it is effectively bypassing and breaking

encryption by working around it, and many of these types of tools involve allowing certain companies access to the server on which private communications are stored.

Schools as the Testbed for the Online Safety Bill

Schools in England and the US have been used on a huge scale as a testbed for the proposed types of “safety” technology during the last decade. The table of “legal but harmful” content in the 2019 White Paper reproduces almost word for word what the school safety tech companies have been monitoring for in the education sector during that time, not only in classrooms, but also at home. This means monitoring not just pupils’ activity, but the activity of anyone when logged into the school network at school or from home. Such technology can be used to monitor all day and every day, even in school holidays.

The Online Safety Bill could be seen as a green light for this kind of monitoring of content which to date has likely been unlawful but never been challenged, and the Bill will inevitably mean wider user surveillance of all digital communications, activity and content. The bill may well emphasise monitoring particular *content*, but that means in the school context, monitoring the *users* of that content and their behaviour. Monitoring has moved away from blocking content and now leads to profiling by design. It sounds good if we know which user appears to be a potential risk to themselves or to others or is interested in potential extremism and terrorism. But why are families and children not told how it works? It's a deeply opaque industry. There is little evidence that MPs generally or policymakers outside the sector understand what they are mandating or how these tools work. They do not understand which companies own them nor which countries they operate from, nor what profiling they do, how the automated decision-making works in those that use AI, nor what records they create about people and who has access to them. Outsourcing to potentially unidentified commercial companies without checks or balances is ineffective, and provides no idea whether monitoring actually works.

There are no safeguards in place about who can set up such a company to monitor children's sensitive online activity. Parental apps technology is widely used by parents, but our research showed that the government's favoured parental app company had not a clue about the legal frameworks they were operating in. The CEO later all but said so publicly himself. The company had developed its child safety app to monitor everything a child

sends, shares or receives without serious independent scrutiny, and was built on an earlier microblogging product.

The danger is that companies who fail to understand or prioritise lawful practice are the very same companies advising the government on what our new laws should be.

What should be required of these systems and companies?

Children have rights set out in law that must be respected to support their full and free development into adulthood, and that includes privacy of communications. But monitoring to find what content children may have or not have access to, may involve monitoring everybody in order to determine who is a child. We should not be mandating more such systems without asking companies to prove they are effective, competent, safe and respect the UN Convention on the Rights of the Child. This includes not only privacy, but the right to be heard, the right to freedom of association, the right to access information, and the right to freedom of expression.

Furthermore, the right to access to justice is really significant when it comes to understanding how children may be affected by terms and conditions, and routes for redress, if what is “lawful but harmful” for children is poorly defined because a lot of their life is spent online.

Not only do we need to understand the full implications of this particular type of legislation and its expansion into the rest of the world. The government is presenting the OSB and its principles as world-leading technology to protect children, but Australia offers a note of caution. Australia had been one of the world's leading countries in Child Online Safety legislation, but just last week delayed its plans around age verification in order to see what happens elsewhere. The Australian government realised that the companies and the technology that they had mandated did not live up to expectations. The Australian realisation suggests we should also reconsider, as the OSB will not respect or support children's safety. Rather, the Bill serves the interests of companies selling questionable technology which could facilitate the creation and distribution of the very content and site-sensitive personal details that these companies claim to prevent.

We need to ensure:

(a) first and foremost, that **private messaging is taken out of scope,**

(b) that proactive or accredited technology has **obligations for oversight and transparency reporting** throughout the life cycle of the product's use, and

(c) that before any such technology is in place, released on the market or brought into law, we should require **independent, published technical assessment** of all tools that monitor and filter digital behaviour, activity or content.

Q&A

Monica Horten: Ella mentioned quite a few issues where there is likely divergence with UK EU law. For example, on the issue of the question of general monitoring, that has dropped out of UK law. The EU has explicitly retained it. You covered two enormously complicated pieces of law, And what the EU is doing. We have Julie Ward here: Julie, that you were the rapporteur or shadow rapporteur on terrorism content regulation when you were an MEP, and I'm curious to hear your responses to what you've heard today.

Julie Ward: I worked on the report. I was tasked with writing an opinion from the culture and education committee. I was trying to stop a lot of this kind of overarching, excessive surveillance at that point. The narrative that Robin gave us at the beginning about what what the British government is doing seems really at odds with any kind of discussion with companies and innovators. That strikes me as being really bizarre for a Conservative Party who claim to be interested in business and innovation.

I just looked at the website for the youth Internet Governance Forum at http://youthigf.com . IGF is the Internet Governance Forum, which happens just for a week, every year, but IGF Youth is 24/7 all year round all across the world. And I think it would be really good for some of the people here to get in touch with IGF youth. Many of these young people are living in quite fragile states, but they really seem to get to grips with the technology and how it can be empowering for them. The issues about children's rights that are coming up, are also really, really important. At the time when I was in the parliament, having these debates in not just in the culture and education committee, but also we would have been having these debates in the children's rights intergroup as well. I was on the steering group of the European Internet Forum which promotes political advocacy for the digital age https://www.internetforum.eu/ and which used to have breakfast meetings with lobbyists from big companies. That is another forum where companies will be putting forward ideas

and trying to win some political concessions from the politicians. I know that IGF youth have been very concerned about this. If you don't already know about IGF Youth, I can put you in touch with the person who runs it, Yuliya Morenets, who is a cybersecurity expert. y.morenets@againstcybercrime.eu

Ella Jakubowska :The Council of the EU's amendments to the CSA Regulation have been described as "terrorist content regulation on steroids" !

Julie Ward: My big demand when working on all these things was always more media and digital literacy to enable users to be more savvy

Robin Wilton: I'm delighted to see that the BCS, too, is calling for a much more holistic and better-targeted approach.

Julie Ward: RT members might like to read this re young people and EU https://northwestbylines.co.uk/news/world/europe/european-parliaments-ambassador-scheme-raises-hope-in-manchester/

Jane Golding: How far is this proposal along in the legislative process and what's the timetable going forward?

Tom Brake: What this excellent webinar shows is how horrendously complicated the OSB is. Is anyone doing any work to try to distil these issues into something the public can grasp and get worried about?

Robin Wilton : I think different civil society groups have got their teeth into specific bits, but the OSB is such an omnibus that it's really hard for a single org to do what you suggest - even though it would be a good idea.

Tom Brake: Unlock Democracy have been following the Online Safety Bill, in a supportive role, for organisations and people like Carl Taylor from FairVote, who's been doing a lot of work on the Bill. But I think what has come across is how extremely complicated the issue is. It was so complicated when it started in Parliament when I was still a member. And I think it has, if anything got even more complicated. And I can see why Members of Parliament will struggle to grasp the different nuances of this. And it is frankly, not landing amongst the general public in any way, while there are very significant implications that most users of WhatsApp, for instance, will not be aware of, so there's a role for organisations like Unlock Democracy and others to try to make this more accessible to the public. And I think that's the big challenge. The level of awareness of it is

very, very small amongst the general public, in comparison like photographic voter ID, where there was a significant degree of awareness amongst the public of the implications. So the question is how do we, how would we raise the profile of it and get people more concerned about it? [Contact: tom.brake@unlockdemocracy.org.uk].

Robin Wilton: A side effect is that UK opposition to the Bill has been frankly limp - in my view, because there's something in there that any given politician wants for themselves…

Tom Brake: A further problem is that it has been going on for so long that everyone but the hard core have lost interest.

Monica Horten: The issue has had very little airtime until fairly recently, when we got a couple of high-profile appearances, we've had Meredith Whittaker [president of the Signal Foundation] on Radio 4 a couple of times, and her Channel Four debate. But really, until then, it has had a very low media profile. And I completely agree, I think it's probably bypassed a lot of the public.

Robin Wilton: I think different civil society groups have got their teeth into specific bits, but the OSB is such an omnibus that it's really hard for a single org to do what you suggest - even though it would be a good idea.

Mark English: I would be interested to know (e-mail mark.english@europeanmovement.co.uk) if the content of the Online Safety Bill could jeopardise the UK's EU data adequacy status? Given that - even if there is content to worry about in the EU legislation - the UK Bill seems to go even further and presumably non-illegal content containing personal data might be shared with UK users and thus become subject to the harmful content provision?

Jo Pye: Civil society groups, including our own, need to come together to discuss their ongoing role in terms of these issues when this Bill becomes law. The Civil Society Alliance (for whom I work) is also interested in promoting discussions.

Jo Pye: Accountability in UK legislation now seems to be in terms of "Trust us, we know what we're doing". Is this an outcome of "We don't need experts"?

Robin Wilton: The list of senior natsec/intelligence professionals whose advice the Govt is disregarding is quite astonishing: Ciaran Martin (ex NCSC), Robert Hannigan (ex GCHQ), Lord Evans (ex MI5)… all say encryption is far more a force for good than bad. Stephen Bonner (ICO): "E2EE [end-to-end encryption] serves an important role both in

safeguarding our privacy and online safety. It strengthens children's online safety by not allowing criminals and abusers to send them harmful content or access their pictures or location."

Robert Hannigan – GCHQ: Encryption on messaging services is "overwhelmingly a good thing" - "it keeps us all safe and secure" - "you can't uninvent it".

Prof Alan Woodward - University of Surrey, ex GCHQ: "So many of us have signed letters, given formal evidence to committees, directly offered to advise - either the government doesn't understand or doesn't want to listen. Ignorance combined with arrogance is a dangerous mix.

"It is not a good idea to weaken security for everybody in order to tackle a minority."

John Gaskell: Regulators are frequently criticised for being toothless. If Ofcom is the 'enforcer' of the Online Safety Bill in the UK, will it have enough, or indeed any, teeth? Or will the OSB be a damp squib?

Robin Wilton: I have heard fairly reliable rumours that Ofcom is looking at these powers with a fair degree of dread. It's not clear to me that it has the resources, technical capabilities or legal bandwidth to be the judge and jury on content at this scale.

Colin Gordon: What we have heard from the panel about the aggressive lobbying of companies offering the EU unproven and questionable solutions chimes with other current stories of post-Brexit government and IT in the UK - notably Palantir's steady conquest of our NHS which is again in the news this week.

Robin Wilton: Correct - both UK and EU policymakers have been assured that the technology to detect illegal material "exists now and is safe and reliable, we're just not making companies use it…". Here's a rebuttal by Ross Anderson: https://arxiv.org/abs/2210.08958

Jen Persson: Further independent review of the UK companies successful in the SafetyTech Challenge found the technology was lacking **:** **https://www.rephrain.ac.uk/safety-tech-challenge-fund/**

Robin Wilton: I haven't said anything about Rejoin, but I entirely share your goals. For more on that topic, you're welcome to follow me at @futureidentity on what remains of Elon Musk's platform…

Lisa Burton - Is there any possibility of stopping, or forcing important amendments to this

Bill in the UK- what can we and the members of our various organisations do?

Colin Gordon: The EU legal office have advised that the mass surveillance provisions of the Regulation would be struck down by the ECJ - is it likely that the EU will go ahead with implementation in face of this finding?

Robin Wilton: I think member states will fall back on the defence that there's a national security requirement here, and therefore powers of mass surveillance would be deployed as a matter of "national competence".

Ella Jakubowska: There have been several official legal opinions saying that the European Court of Justice would likely strike down this proposal, but for some reason that has not bothered the European Commission.
And the Council of EU member state governments have said they will disregard the legal advice and try their luck with the court!

Jo Pye: "AI" is the tsunami waiting to complicate everything. Just how is personal/human impersonation going to be investigated and "punished"?

Robin Wilton - It's very hard to see how, especially at the scale at which AI is expected to generate "abusive content that does not portray an actual human individual".

Jo Pye: Once again, Both EU and UK are going to depend on a "Good Chap Model". But who are the "Good Chaps"?

Robin Wilton: Fair comment, Jo. At least in the EU the bedrock is still assumed to be respect for fundamental rights - whereas here, our Government seems keen to do all it can to escape that obligation.

Robin Wilton: The economic aspects Ella mentions are really not visible **at all** in the UK policy debate. There's little or no understanding of the economic forces that enable or encourage illegal content, and therefore little appreciation of how to counter them.

Additional materials and links shared during the session.

Robin Wilton:
The CRIN report Jen mentions is excellent - highly commended.
https://home.crin.org/readlistenwatch/stories/privacy-and-protection

The BCS has also just published a short analysis of the Bill's implications:
https://www.bcs.org/articles-opinion-and-research/online-safety-bill-shouldn-t-rely-on-

technology-to-deliver-child-protection/

Here's the 'mythbuster' on the government's claim that they "aren't breaking encryption": https://www.internetsociety.org/resources/doc/2020/fact-sheet-client-side-scanning/

And here is the UNICEF 2-pager on children's rights in this context: https://www.unicef-irc.org/publications/1152-encryption-privacy-and-childrens-right-to-protection-from-harm.html

Patrick Breyer MEP's page on "chat control": https://www.patrick-breyer.de/en/posts/messaging-and-chat-control/

Ella Jakubowska :
This is the event Monica mentioned, where we will discuss the importance of encryption: https://edri.org/take-action/events/save-the-date-join-edri-to-talk-encryption-surveillance-and-privacy/

If you would like to come, please contact me at ella.jakubowska@edri.org and I will send you an invitation

And if you'd like to see all the criticism of the EU's CSA Regulation proposal, you can find it here: https://edri.org/our-work/most-criticised-eu-law-of-all-time/

Online Safety Bill: Postscript and update.

Robin Wilton wrote [06 09 2023]:

I mentioned the absurdity of the Online Safety Bill's reference to "accredited technologies", and if the attached article is to be believed, that very absurdity may now be the thing that is giving the Government enough ambiguous "wriggle room" to claim that the Bill won't put people's privacy at risk as long as the technologies in question continue to be imaginary…

It doesn't **feel** very much like a resounding victory for the pro-encryption advocates, but if that's how it turns out, I won't complain.

<< POLITICO Pro Alert

UK seeks to allay concerns over encryption powers as campaigners claim victory
By Laurie Clarke · Sep 6, 2023, 6:39 PM ·

LONDON — Lords Minister Stephen Parkinson has made a statement in the Commons attempting to allay concerns over controversial powers in the government's Online Safety

Bill which critics say give Ofcom unprecedented powers to break encryption.

“There is, let me be clear, no intention by the government to weaken encryption technology used by platforms, and we’ve built strong safeguards into the bill to ensure that users’ privacy is protected,” Parkinson told the chamber on Wednesday afternoon.

The minister said that Ofcom would have to comply with existing data protection legislation, as well as the Human Rights Act 1998 and the European Convention on Human Rights, when issuing a notice under clause 122 of the bill.

That clause, which allows the regulator to mandate services to use “accredited” tools to spot child sexual abuse or terrorist content on their platforms, also states that Ofcom must first commission a “skilled person’s report” and have regard to the impact of the power on users’ privacy and free speech.

“If appropriate technology does not exist which meets these requirements, Ofcom cannot require its use. That is why the powers include the ability for Ofcom to require companies to make best endeavours to develop a new solution,” he clarified.

But Parkinson was pipped to the post by a Financial Times article that framed part of his statement – saying that an Ofcom notice can only be issued “where technically feasible and where technology has been accredited as meeting minimum standards of accuracy” – as the government backing down in the face of tech company pressure.

However, Parkinson has made similar comments in the House of Lords before.

“Ofcom can require the use of technology on an end-to-end encrypted service only when it is technically feasible and has been assessed as meeting minimum standards of accuracy,” he said on the final day of report stage in the Lords on July 19.

“If it is not proportionate or technically feasible for companies to identify child sexual exploitation abuse content on their platform while upholding users’ right to privacy, Ofcom cannot require it,” he also said in July.

The government refutes the Financial Times’ framing that it has backed down on the issue.

“Our position on this matter has not changed and it is wrong to suggest otherwise,” said a government spokesperson. “Our stance on tackling child sexual abuse online remains firm, and we have always been clear that the bill takes a measured, evidence-based approach to doing so.

“As has always been the case, as a last resort, on a case-by-case basis and only when

stringent privacy safeguards have been met, it will enable Ofcom to direct companies to either use, or make best efforts to develop or source, technology to identify and remove illegal child sexual abuse content – which we know can be developed."

Nevertheless, the statement, which follows months of lobbying and threats by major platforms to withdraw their services from the U.K., prompted celebratory statements from those engaged in fighting this part of the bill.

"I'm so moved, a bit stunned, and more than anything sincerely grateful to those who came together to ensure sunlight on the dangerous OSB Spy Clause, and to those in the UK gov who synthesized the facts and acted on them," tweeted Signal's Meredith Whittaker. "I knew we had to fight. I didn't know we'd win." >>

Here is a selection of other reports and commentary on recent developments in the passage of the Online Safety Bill.

https://www.ft.com/content/770e58b1-a299-4b7b-a129-bded649a43b
http://www.iptegrity.com/index.php/digital-britain/onlinesafetybill/1156-online-safety-bill-ray-of-hope-for-free-speech - Dr Monica Horten
://www.iptegrity.com/index.php/digital-britain/onlinesafetybill/1157-online-safety-bill-passes-as-us-court-blocks-age-checks-law - Dr Monica Horten

https://twitter.com/Iptegrity/status/1699753307600834683?s=20

https://www.politicshome.com/news/article/labour-party-charities-fear-online-safety-bill-left-huge-gaps

https://www.openrightsgroup.org/blog/omnishambles-over-encrypted-messages-continues/

https://www.techradar.com/pro/security/the-online-safety-bill-is-just-the-tip-of-the-uk-surveillance-state-iceberg

https://www.businesstelegraph.co.uk/the-online-safety-bill-is-just-the-tip-of-the-uk-surveillance-state-techradar/

https://www.eff.org/deeplinks/2023/09/uk-online-safety-bill-will-mandate-dangerous-age-verification-much-web
https://www.spectator.co.uk/podcast/silkie-carlo-is-the-uk-the-next-surveillance-state/

https://www.wired-gov.net/wg/news.nsf/articles/techuk+statement+on+the+online+safety+bill+14092023130500?open

https://www.indexoncensorship.org/2023/09/online-safety-bill-loophole-opens-door-to-unprecedented-investigatory-powers/

https://www.computerworld.com/article/3706810/uks-controversial-online-safety-bill-set-to-become-law.html

https://www.nytimes.com/2023/09/19/technology/britain-online-safety-law.html

https://blogs.bournemouth.ac.uk/research/2023/09/28/conversation-article-online-safety-bill-why-making-the-uk-the-safest-place-to-go-online-is-not-as-easy-as-the-government-claims/

https://www.newscientist.com/article/2393012-uks-online-safety-bill-to-become-law-but-can-it-be-enforced/ by Matthew Sparkes

https://bigbrotherwatch.org.uk/2023/10/five-things-you-need-to-know-about-the-online-safety-bill/ by Mark Johnston

Participants

Chair
Dr Monica Horten

Speakers
Ella Jakubowska (EDRi)
Jen Persson / Defend Digital Me
Robin Wilton

Tom Brake
Lisa Burton
Mark English
John Gaskell
Jane Golding
Monique Hawkins
Mark Johnston
Sharon Leclercq-Spooner
Julie Ward
Irina von Wiese
Paul Willner
Kate Willoughby

Round Table Team
Colin Gordon
Helen Grogan
Jonathan Harris
Caroline Kuipers

Juliet Lodge
Lilian McCobb
Tony McCobb
Jo Pye
Magdalena Williams

Next Sessions:

Tuesday November 7th, 5pm - 6:30pm – details shortly.

Tuesday December 5th, 5pm - 6:30pm – details shortly.