November 7, 2023

Dear Supervisor Wiewiórowski,

I was unable to participate in the seminar hosted by the European Data Protection Supervisor (EDPS) on October 23 due to a mild illness. So instead I'm sharing my planned remarks here.

First, I want to express my appreciation to you, Supervisor Wiewiórowski, for convening what I understand was an excellent–and in the context of the regulation being considered–unprecedented event.

It should not be remarkable that experts with domain knowledge of computational systems, their political economic drivers, and the intersection between human rights and networked services have finally been welcomed into the room. Nor that they are being listened to. Indeed, one would be forgiven for assuming that such expertise would be the bedrock of any regulatory proposal. Sadly this is not always the case, particularly in the context of this Bill. The absence of experts' advice, as well as the flagrant disregard for scientific consensus has been a hallmark of the CSAM legislation currently under consideration.

But truth has a way of finding the light. In spite of some Commissioners' apparent allergy to expertise, experts spoke out, and growing public awareness followed. An understanding of just how technologically and politically unworkable the current CSAM proposal is has become common sense, even as those behind the Bill continue to evade and avoid this reality. Make no mistake: children must be protected, and rights must be preserved. But the CSAM proposal in its current form does neither.

When I first learned about this proposal I admit I was confused. Europe prides itself on being a bastion of rights, foregrounding privacy well ahead of the US, where I'm from. It was only after rigorous investigative reporting illuminated the private lobbying that shaped the CSAM proposal in the interests of organizations selling their own tech solutions that I fully appreciated what had happened.

Put simply, organizations that sell surveillance tools as a remedy to the social problems of child abuse and exploitation had been in the driver's seat, crafting the Bill's legislative mandates in order to position their products as the solution.

Commissioners colluding with these organizations appear to have placed the organizations' word above that of respected child advocates on the ground.[1] In doing so, they ignored technical experts and human rights groups who warned that such "solutions" are in fact magical thinking and tech hype–and if implemented would undermine safety, rights, and liberties.

That such naked profiteering was permitted at such high levels in Europe surprised me. I have seen this practice for years in the US, where large tech companies spend hundreds of millions influencing legislation and boxing out expertise and public interest.[2] The further revelations that the proposal's advocates within the Commission engaged in privacy-invasive ad microtargeting–which may itself be a violation of EU law–is a level of messy hypocrisy that is hard to fathom.

These revelations of self-interested tech industry pressure shaping this Bill with willing participation from some Commissioners, alongside the longstanding expert consensus impugning the Bill's feasibility and legality, in addition to the concerns that EDPS have surfaced, raises the serious question: *why are we still here?*

How is it possible that despite clear warnings about the proposal's threats to fundamental rights, its technical infeasibility, and the documented corruption that has dominated its creation and propulsion, the CSAM regulation is *still* moving through the legislative process?

Where is the pause for a reset, for due diligence, for judicial review, and above all, for a full and objective investigation of Commissioner Johansson's involvement and her entanglement with interested tech organizations?

We can perhaps find an answer to this question by reflecting on my recent experience in the UK, where I engaged with policymakers on the risks to end-to-end encryption posed by the Online Safety Act. As in the EU, the UK public is deeply aware of the dangers that the mass surveillance posed by this legislation presents. We saw how the government tied itself in rhetorical knots, resorting to magical thinking and incomprehensible claims to argue that the experts were wrong, and that through the power of "AI" it would be possible to scan everyone's end-to-end encrypted personal communications, privately. Such technologies do not actually exist. But this didn't stop the inertia propelling the Act's backers. We also saw how the Act acrimoniously divided the government itself, and

---

[1] For example, Offlimits, Europe's oldest hotline for reporting child abuse, attempted to initiate contact but were unable to access Johansson. See: https://balkaninsight.com/2023/09/25/who-benefits-inside-the-eus-fight-over-scanning-for-child-sex-content/

[2] One example among many can be found in Microsoft influencing–even writing parts of–facial recognition laws that have gone into place across US states. While community groups and civil liberties advocates advocated for stronger laws, Microsoft was able to weaken these considerably, drafting what are ultimately extremely permissive guardrails that enable the mass deployment of facial recognition. See: https://qz.com/1905159/microsoft-is-shaping-facial-recognition-bills-across-the-us

triggered substantial anger towards the ruling Conservative Party which created the legislation. This anger is already costing them seats.[3]

Ultimately, after significant public pressure, the government was forced to concede that the technology the Act depends on to be comprehensible does not in fact exist. Yet despite this acknowledgement, despite the public pressure, and despite clear expert testimony, the law was pushed through. Too many policymakers, advocates, and campaigners had invested too many years, too much work, and too much money into the law to turn back. Too many people had staked too many outcomes on the law's existence. And too many reputations were riding on it. No one, from any party or faction, had the courage or the integrity to say stop.

Allowing the sunk cost fallacy to trump technical, political, legal, and social concerns is a dereliction of duty that should haunt any lawmaker whose legacy it now stains. This is how the UK has been left with a package of unworkable, burdensome, intrusive, and technically infeasible legislation. This law will not solve the problems it was conceived to solve–indeed, by drawing attention and resources away from evidence-based solutions, it could arguably exacerbate these problems. But it will expand dangerous surveillance powers, undermine human rights, and further isolate the UK and its economy.

There is one more lesson to take from the UK. We need only reference the work by the REPHRAIN Centre at the University of Bristol, which was appointed by the UK government to review scanning technologies funded by the UK's Home Office. REPHRAIN found that *every single project* piloted for the UK's Safety Tech Challenge project–a government initiative designed to create a lucrative marketplace of vendors for companies to choose from to meet their compliance obligations–*violated fundamental rights and freedoms.*

I ask the EU to please learn from the UK's mistakes and heed these lessons before it's too late. If the EU does not, and if the flawed CSAM proposal is rammed through in spite of the conflicted, compromised mess that we know it to be, it will be a very grim day for Europe.

European law enforcement agencies are already overwhelmed with false positive images reported under current temporary legislation, including images exchanged privately between individuals in the context of their personal consensual relationships. Even putting aside the technical infeasibility of the law, and the profound human rights concerns it raises, it would be folly to move forward with legislation that would exponentially increase that problem before solving it first: if you are looking for a needle in a haystack, the solution is not to make the haystack bigger.

That testimony shows that even today, millions of innocuous images are being caught in the AI scanning net, with few ways to sort and act on them. Breaking end-to-end

[3] Following her resignation as a Member of Parliament, a byelection saw the constituency seat which had been held by the Minister for Digital who shepherded the regulation flip to the opposition party for the first time since 1931. https://www.bbc.co.uk/news/uk-england-beds-bucks-herts-67147435

encryption, one of the only technological safeguards we have to ensure meaningful private communications, would foolishly eviscerate privacy for journalists, dissidents, human rights activists, and anyone else in the EU, and anyone they communicated with.

My request to policymakers in Brussels and beyond is this: have the courage to grapple with the facts, and have the strength to stop bad legislation before it's too late. Today is an opportunity for learning and dialogue: we, and all the other groups represented at the seminar, stand ready to work with you in good faith to map the political, legal, social, and technical risks that the CSAM proposal carries. Do not prioritize the sunk cost fallacy over fundamental rights and technical feasibility. Commit to recentering human and children's rights in your legislative endeavors in ways that will preserve the integrity of Europe's rights-based system. Refocus your efforts on pursuing harmful business models, whether they come from big tech platforms or from enterprising AI vendors keen to shape legislation around their business models. And above all, commit to protecting end-to-end encryption in whatever form the proposal takes.

Warmly,

Meredith Whittaker
President, Signal