The speech of Meredith Whittaker, Signal Foundation's President, at the EDRi-organised event on encryption in Brussels (26 September 2023)

As you're aware, we are in the midst of a storm of global attacks on the human right to privacy– with governments, security services, NGOs that double as AI companies, and a lot of money and too little transparency hard at work trying to walk back the few safe havens we've been able to carve out against the ferocious surveillance business model and the states that skim off of it.

I've been in tech for almost twenty years, and I've worked on issues relating to privacy on and off throughout. I have watched many government challenges to encryption. But I have never seen anything as willfully misleading as the campaign I'm seeing now.

I just came from the UK, which is leading the charge against encryption and the right to privacy. What I witnessed there is alarming. Anti-intellectualism and propaganda define both the popular, and even much of the so-called expert discussion. An air of hysteria and menace hangs over any attempt at meaningful discussion, including discussion of evidenced approaches to help children that diverge from the fixation on online surveillance. And this makes it scary and difficult to defend human rights, when the implication is that in doing so you're defending demons and monsters. Under these harsh conditions, democratic deliberation over this incredibly serious affront to rights was stunted. And I don't believe this was accidental.

This air of hysteria provides cover for the uncomfortable fact that the tech to do the thing they're legislating *does not exist in any workable form*. In spite of what the organizations marketing it claim, it is not possible to scan everyone's e2ee communications in order to flag banned expression safely and privately. To say otherwise is magical thinking.

But even under these conditions, many in the UK did speak up to say as much. The human rights community, the academic expert community, civil rights organizations, and many others in the UK were vocal in the leadup to the Bill's passage. Amnesty made clear that their global work would be endangered by any move to undermine end to end encryption. Since communication does not stay within a given jurisdiction, vulnerable people living under authoritarian surveillance whom Amnesty communicates with and helps would also be at risk, stripped of their privacy and exposed. Stonewall, an LGBTQ advocacy and service organization, made a similar point, referencing their global work and the 64 countries in which LGBTQ identity is criminalized. And many familiar with Ukraine, whose government uses Signal as core communications infrastructure, expressed similar alarm.

A united chorus of experts also spoke to the misguided marketing and AI hype on which the bill's assumptions about scanning e2ee were based. The REPHRAIN independent research center, which was appointed by the UK government to review AI scanning prototypes proposed for such

use, took the highly unorthodox step of declaring that these tools were not fit for purpose, echoing long standing expert consensus. Even Apple Inc, the trillion dollar market cap monopoly that in 2021 briefly deployed client side scanning for encrypted data before their system was found to include serious vulnerabilities, came out publicly and said that, having tried it, they now recognize that it is not possible to build such a system that is both private and secure. Indeed, by the end of the process, even *the UK government itself* was forced to acknowledge that no tech exists that can safely and privately scan e2ee communications.

What was chilling to me is that even with the UK government's acknowledgement, the bill moved forward. Multiple people I spoke with in government simply waved their hands – political inertia would proceed irrespective of the dangers, damages, and folly, they said, looking into the middle distance. We were told that the Home Office wanted this bill and the power it gave them to undermine encryption. So even with the pretext eroding, with the claims being fact checked into oblivion, the bill moved. And in the process, it exposed serious cracks in the UK's democratic foundations.

The EU has a chance to stop this tide, and to turn away from the absurdity that defined this in the UK. And if it doesn't, I don't really know what we'll do, because the EU's stamp of approval on such a profound setback to human rights–and such a significant endorsement of Big Tech-style surveillance–would open the door for everyone else.

I don't come from a country where we can trust our institutions with the peace of mind that you do here. In the US, a woman named Jessica Burgess and her daughter are now in prison, having been sentenced to a felony for accessing criminalized reproductive care in the state of Nebraska following the Supreme Court decision. Facebook messages, turned over by the company, were key evidence used to convict Jessica and her daughter. A wave of book banning continues to sweep many US states, while a law in Florida proposed that any journalist covering local politics be forced to register with the state. And Senator Marsha Blackburn recently suggested that scanning similar to that being proposed in the EU should be expanded to include LGBTQ+ content. The slippery slope is not hypothetical to me.

This is not to say that the EU should be entirely trusting of its institutions, either. Wherever these laws are being pushed, there are many interested tech companies (some posing as NGOs) and governmental departments that cannot wait to expand their profits and/or power. According to recent investigative reporting, EUROPOL is already making the case for expanding scanning to the Commission, saying "there are other crime areas that would benefit from detection." According to meeting minutes, the response from commissioners was not horror, but what appears to be a note of strategic caution, telling EUROPOL that it, "needs to be realistic in terms of what could be expected, given the many sensitivities around the proposal."

Now, if institutional wariness is warranted in the context of government, suspicion of the companies peddling AI hype as a way to solve harm to children is downright required. It's deeply ironic that the same government that is pushing to lead on meaningful AI regulation, with the AI Act and DMA, is also falling for baseless AI hype when it comes to children. And yes, AI hype is the most accurate description of the marketing and unsubstantiated claims being made about client side scanning for e2ee.

Just last week, the AI company and NGO Thorne pitched a webinar to market AI tech for undermining e2ee to EU politicians, with a whole session dedicated to bringing AI company CEOs to discuss, "solutions to detect in end-to-end encrypted environments." Because this was framed as an intervention to protect children, it is not treated with the skepticism that meets most other tech lobbying. DragonFlAI, one of the companies invited to market their tech in the webinar, has ties to biometrics giant Yoti. DragonFlAI claimed, without evidence, that their tech "allows nudity and age to be detected together within e2ee." Now, again, no such tech exists that can do this. The tech that's been built – INCLUDING DragonFlAI's products–have been panned as unworkable, error filled, and ultimately unsafe and privacy invasive.

The companies peddling these services are selling technical solutions to social problems (and offering the security services a much covered backdoor to e2ee in the process). They marshall millions of dollars to shape the political process to an alarming degree, and in the case of the EU, according to recent reporting, some members of government are willing participants, collaborating with these companies and their networks in highly conflicted ways.

It doesn't matter how many times you say it – AI is not conscious, it's not superhuman, and AI-based scanning cannot both maintain privacy and security and surveil all private communications. It is the regulator's job to understand this.

With the smoke clearing, and the financial influence of those pushing to undermine encryption for profit and power becoming clearer, I am cautiously hopeful that the EU can be where this wave of attack stops. Because if this wave of legislation takes hold beyond the UK, it's not clear that Signal could survive. Just as our commitment to provide a tool for meaningful private communication does not change based on region, our position on this legislation does not change. We are a nonprofit, which means we can be laser focused on our principles and mission, without shareholders or VCs pushing us to compromise.

As in the UK, as in Iran, as everywhere: we will continue to do everything in our power to ensure that people in the EU have access to Signal and to private communications. But *we will not* undermine or compromise the privacy and safety commitments we make to people in the EU, and everywhere else in the world. And we will never install a backdoor or otherwise undermine the encryption that keep the people who use Signal safe. We would rather leave.

I want to close by thanking EDRI for their hard and essential work, and for doing this work in the face of such cynical rhetoric. There’s hard work to be done, but I believe when the facts are clear and public, we can win.