President of Signal Foundation Meredith Whittaker's speech for EDRi's 20th anniversary

Thank you so much, It's a great honor to be here with EDRI, who do incredible work ensuring that flashy claims from tech companies and celebrities don't succeed in distracting us from what's important – a livable future grounded in the preservation of fundamental rights. EDRI is a model for coalitional work that takes its goals seriously, and I sleep better at night knowing you all are here. So thank you, and happy birthday.

But I want to use this talk to discuss some of what keeps me up at night – particularly the recent spate of regulatory proposals and misguided tech fixes that offer false and surveillant solutions to complex social problems – solutions that always seem to lump the right to privacy in with malfeasance, and offer to address bad actions by eliminating privacy.

Make no mistake – these proposals are grave attacks on everything Signal does and stands for. Signal exists to provide tools for private communication in a world increasingly shot through with surveillance. We do this by tirelessly developing and maintaining the Signal messenger app – the only messenger endorsed by the European Commission – and by devoting resources toward research that we share beyond Signal to improve privacy for the ecosystem overall.

In 2013, the Signal Protocol introduced a significant advancement in communications privacy, and has become the standard for messaging privacy, used by multiple other apps. Billions of messages are encrypted using the Signal protocol every day. Beyond this, Signal has also developed novel technology that protects identity and metadata, which we implement to ensure that the Signal Messenger app provides truly robust privacy.

I could talk about the nuances of our technology and its implementation all day. But sadly today we have other work to do, and other battles to fight.

During my almost 20 years in tech, I've seen the same conversations emerge, die down and reemerge, and the same kind of magical thinking crop up over and over again.

The pattern goes something like this: a complex and harrowing social problem receives attention from regulators and media. Everyone acknowledges the gravity of the problem and the urgency of addressing it. We feel distressed, concerned, and emotional, and people rush to "do something."

Over and over again we're presented with the same specious "solutions". To right the wrongs of a troubled world, the refrain goes, private communication must be curtailed.

Of course, the history of computation is littered with cautionary tales of the dangers of mass surveillance – from the Nazi's use of IBM's Hollerith machines to organize genocide, to the US illegally accessing its census data to identify and inter Japanese Americans during that same period, to South Africa's aspirations to digitize enforcement of apartheid segregation, into today,

which sees large tech companies handing over the data of people seeking criminalized medical care in the US.

But I don't think I have to dwell on these histories here. Those in this room know the dangers of mass surveillance, especially in authoritarian times.

Similarly, the history of communications technology is littered with the magical thinking of governments that have tried and failed to have their cake and eat it – to create backdoors that can only be accessed by "the good guys" while remaining secure against threats from "everyone else."

And these efforts have persistently failed. The infamous Clipper Chip is only one example. Millions of dollars have been spent on dead ends, and projects shelved over and over again. Because the truth is that any scheme that provides access for "us" can just as quickly be exploited by "them" – hostile actors eager to compromise critical infrastructures on which the government, economy, and civic institutions rely.

Nonetheless, we see this strain of magical thinking reemerging with a vengeance, in the UK's misguided Online Safety Bill provisions, in the EU's chat control regulation, and the data retention struggles happening at a country-level, like Belgium's encryption crackdown and debates about whether bulk retention of private communications is permissible or wise.

Now not all of these proposals say the word "backdoor" out loud. Indeed, such proposals have become more sophisticated in the last years, at least in their language and framing. Like the EU CSAM legislation, many claim without evidence that what they propose is compatible with end to end encryption, even as they mandate practices that would be impossible to implement without weakening or eliminating end to end encryption. This is like a boss giving an employee two days worth of work to complete and saying "I would never force you to work for two days straight, I am just telling you to complete this all in one day." It's not possible, and saying it is doesn't change that.

Others propose an equally dangerous but more novel variant of magical thinking. They concede that backdoors aren't the way forward. Instead, they suggest mass surveillance "outside" of end to end encryption, generally pointing to client-side scanning systems. Don't worry, these proponents assure us, we will scan your messages on your device before they're encrypted, checking them against opaque databases of banned speech to ensure that you're staying within government-approved boundaries of expression. After that? Sure, go ahead and encrypt.

Client side scanning is a faustian bargain that nullifies the entire premise of end to end encryption by mandating deeply insecure technology that would enable the government to literally check every utterance before it is expressed.

CSS poses other problems. It also creates new vulnerabilities that carry with them many of the same security and safety issues that come with weakening encryption.These systems rely on

so-called AI, technology that produces significant false positives and can be hacked through adversarial attacks for which there are few defenses. Indeed, the EU is in the midst of negotiating their AI law in response to these very challenges. On that note I think it's imperative that we bring the people who have been carefully researching the flaws and fallibilities of AI systems to the discussion about client side scanning, and recognize that here, as elsewhere, AI is not a silver bullet.

I'll also note that it's been surprising and perplexing to hear celebrities and influencers, not to mention politicians, claim that technological solutions exist that can scan content for forbidden expression without breaking end to end encryption. I'm not a celebrity or an influencer, but I do know tech, and I will state for the record that there is no such thing. It's simply not possible. And either these people are badly misinformed, in a deep and concerning state of denial, or dangerously cynical – hoping that by promising a nonsense tech solution they will get laws passed and implement surveillance before anyone is the wiser.

A world where privacy is eliminated is a world where power asymmetries are locked in amber, where dissent becomes dangerous, intimacy risky, and where the muscles for exploring new ideas, asking beginner's questions, or working through inchoate musings atrophy.

This, again, is why I am grateful to EDRI for your work. These are not dry, technical issues that belong in a sidebar on tech policy at some dreary meeting. These are fundamental to a livable future. And right now we're facing a renewed and vitriolic attack on privacy that will take real resolve to contest.

When encryption is broken in a world so reliant on digital communications, the fundamental right to privacy is all-but washed away, along with the security and robustness of the digital infrastructures that commerce, government, and civil society rely on.

In Hungary, gay and trans people are being singled out and criminalized, alongside LGBTQ literature and expression. In the US, where I live, we have a proposed law in the state of South Carolina that would punish people with the death penalty for receiving criminalized reproductive healthcare. And across the states we're seeing proposals to criminalize same sex marriage, with some even floating a ban on interracial marriage. Why do I mention these? Because in the future too many want, this is the banned expression, the forbidden love, the impermissible identities that your client side scanning would be tasked to detect, that your magical backdoors will be used to suss out, that your regime of bulk mass surveillance will be applied to punish.

Jessica Burgess, a 41 year old mother from Nebraska, already knows some of this future. In 2022, Facebook handed messages between Jessica and her daughter to law enforcement. And these were used to charge her with a felony for helping her daughter get reproductive healthcare in a state where such care had been made suddenly illegal.

It's time to come back to reality. Complex social problems absolutely need serious redress. But using these problems as emotionally evocative pretexts to justify the elimination of privacy will

not solve them. Indeed, the measures being considered in Europe, the UK, and beyond – however noble the language justifying them appears – will pave the way for dark futures.

With that, I'll close by saying that I'm proud to stand with you all, and I'm proud to work everyday to ensure that private, safe and intimate communication remains accessible to everyone. And again I want to thank EDRI members for your invaluable and tireless work, and to wish you a very happy birthday.