The fight over encrypted messaging is just beginning

In October, a group of top elected officials in western democracies wrote to Facebook expressing concern about the company's plans to incorporate end-to-end encryption in all of its messaging products. US Attorney General Bill Barr, along with his rough equivalents in the United Kingdom and Australia, wrote that encryption would make it difficult or impossible for them to uncover instances where messaging was used to facilitate terrorism, child exploitation, and other crimes. They asked Facebook to reconsider its plans.

Anyway, the company thought about it and the answer is no. Here are WhatsApp chief Will Cathcart and Messenger honcho Stan Chudnovsky (in a PDF! sorry):

> *Cybersecurity experts have repeatedly proven that when you weaken any part of an encrypted system, you weaken it for everyone, everywhere. The 'backdoor' access you are demanding for law enforcement would be a gift to criminals, hackers and repressive regimes, creating a way for them to enter our systems and leaving every person on our platforms more vulnerable to real-life harm. It is simply impossible to create such a backdoor for one purpose and not expect others to try and open it. People's private messages would be less secure and the real winners would be anyone seeking to take advantage of that weakened security. That is not something we are prepared to do.*

The letter goes on to note ways in which Facebook does work with law enforcement, and says it continues to develop ways to detect and monitor bad actors on Facebook products without

breaking encryption.

This is the right approach to take, in my view, even if in some ways it's self-serving for Facebook. The company is shifting to private messaging because its users had already started without them; its chief rival in America, iCloud, had already set end-to-end encryption as the privacy standard; and by taking up this fight, Facebook can cast itself in the role of noble privacy defender. (There are downsides, too, of course: a terrorist act planned on WhatsApp is going to be a public-relations catastrophe no matter how much people love their privacy; and in the meantime plenty of lawmakers will be lining up to cast Facebook as an enemy of the people.)

Speaking of which: Lawmakers thought over this answer during a Senate hearing today, and you probably will not be surprised to learn that they are not satisfied:

> *Lawmakers of both parties echoed those worries on Tuesday, threatening to take action if the companies didn't satisfy their concerns.*
>
> *"You're going to find a way to do this, or we're going to do this for you," said Senator Lindsey Graham, Republican of South Carolina and the chairman of the Judiciary Committee. "You're either the solution or you're the problem."*

This sort of quote used to impress me much more before lawmakers started saying a version of it in every tech hearing since 2017. I used to think that they meant it, but at some point I realized that threatening tech regulation is what American lawmakers generally do instead of passing laws.

Other countries do actually pass tech regulations, of course, for better and for worse. Australia famously passed a law last year mandate that companies break encryption upon request. (It appears not to have been tested yet? But let me know if I missed something.) The Trump Administration under Barr has

recently proposed exploring similar requirements.

One reason that civil liberties groups (and me) tend to oppose proposals like this is that while governments talk a big game about using these tools to fight crime, they also typically use these tools to surveil citizens and journalists. For example, here's something that's happening in Australia:

> *Data retention legislation passed in 2015 had a carve-out for journalists that required law enforcement to obtain a special journalist information warrant, but Pfefferkorn said in a personal submission to the review that the combination of the new powers meant the information warrant need not be obtained.*
>
> *"Law enforcement's powers granted under the Data Retention Act in 2015 were augmented by the new powers the Assistance and Access Act provided at the end of 2018, creating the framework that authorised the federal police in mid-2019 to raid the homes and offices of journalists over articles published in July 2017 and April 2018, in defiance of international norms," she said. "Because parliament passed these laws, the federal police had the power to strike a chilling blow against press freedom in Australia, and call it lawful."*

Would Americans implement the law any differently? Well, here's a Reuters investigation published today about former U.S. counterterrorism czar Richard Clarke, and how he and former White House and U.S. defense executives worked to build a surveillance empire for the government of the United Arab Emirates. Note how the stated purpose of the surveillance — to catch and stop extremists from carrying out acts of terrorism — quickly expands to include good old-fashioned harassment of government critics:

> *In the years that followed, the UAE unit expanded its hunt far beyond suspected extremists to include a Saudi women's*

> *rights activist, diplomats at the United Nations and personnel at FIFA, the world soccer body. By 2012, the program would be known among its American operatives by a codename: Project Raven.*
>
> *Reuters reports this year revealed how a group of former National Security Agency operatives and other elite American intelligence veterans helped the UAE spy on a wide range of targets through the previously undisclosed program — from terrorists to human rights activists, journalists and dissidents.*

My personal feeling about end-to-end encryption is that it should be available to citizens for one-to-one communication, but not for one-to-many communication. So encrypted WhatsApp should exist, but you shouldn't be able to infinitely forward encrypted WhatsApp messages. (You cannot currently do that in WhatsApp.) The very real downside here is that criminals will exploit the availability of encryption to plan crimes. But the upside is that hundreds of millions of law-abiding citizens will have a safe space to communicate in a world that is increasingly defined by surveillance and monitoring technologies.

The ability to speak freely, and privately, in a world where democracy is in decline seems vital to me. I only hope it seems as vital to the electorates of Western nations, who will likely have to lobby lawmakers to preserve these freedoms. The fight over encryption has now begun in earnest, and the survival of private messaging is far from assured.

The Ratio

Today in news that could affect public perception of the big tech platforms.

Trending down: The US National Labor Relations Board has begun

an official investigation into **Google** after the recent firing of four employees. It's also looking at whether the company discouraged employees from engaging in union activity.

Trending down: Facebook's advertising tools may be more responsible for the polarization of American politics than previously understood. New research shows a skew in the delivery of political ads based on the content of those ads alone, rather than the targeting decisions made by political campaigns. The gist: it's more expensive to talk to people who disagree with you.

Governing

 In the United Kingdom, politicians are using disinformation techniques to grab attention, distract the news media, stoke outrage and rally support. The trend could be a preview of what's to come in the United States as more public figures engage in misinformation to compete with **President Trump.** Adam Satariano and Amie Tsang at *The New York Times* explain:

> *Polls suggest that voters are shrugging off accusations of online trickery, as Facebook has said it will not screen political ads for accuracy. Experts said this means the tactics were likely to further enter the mainstream in Britain and elsewhere.*
>
> *"This is the election where disinformation was normalized," Mr. Davey said. "A few years ago people were looking for a massive coordinated campaign from a hostile state actor. Now, many more actors are getting involved."*

TikTok chief Alex Zhu canceled a scheduled trip to Washington to meet with members of Congress. The move stoked fresh criticism of the social-media app at a moment when it's trying to repair its relationships with US officials. (Tony Romm / *The Washington Post*)

YouTube asked the Federal Trade Commission to eliminate rules that assume anyone watching child-oriented content is under 13 and thus ineligible to be shown ads. The agency is currently revamping privacy regulations that could have a sweeping impact on the video sharing platform. (Ben Brody and Mark Bergen / Bloomberg)

Major nonprofits have pledged millions of dollars to take on Big Tech. One of the groups receiving foundation money is led by **Chris Hughes**, a **Facebook** co-founder who now publicly argues for breaking up the social media giant. (David McCabe / *The New York Times*)

A social media influencer has been sentenced to 14 years in federal prison for concocting a violent scheme to coerce a stranger into giving up a web domain name. The scheme involved holding the domain owner at gunpoint. Also available as a longread in *One Zero*! (Nick Statt / *The Verge*)

States are struggling to pass strong privacy legislation. Following the **Cambridge Analytica** scandal and the California Consumer Privacy Act, many attempted to pass laws that would give people more control over their data. But pushback from the tech and telecom industry has slowed these efforts. (Ashley Gold / *The Information*)

India proposed groundbreaking new rules that would require companies to get consent before collecting peoples' personal data. The law would also force companies to hand over "non-personal" user data to the government. (Manish Singh / *TechCrunch*)

Industry

Facebook's Oculus Quest VR headset is becoming the first VR system with native hand tracking. Starting this week, VR users will be able to put down their controllers and use their fingers to manipulate VR worlds, as tracked by Quest's array

of built-in cameras. Sam Machkovech at *Ars Technica* tells us why this is a pivotal moment for VR:

> *Normally in VR, users grab onto controllers full of triggers and buttons. For some VR software, a piece of handheld plastic makes sense: it can sell the sensation of holding a weapon or VR item, and it adds haptic feedback like rumbling when your real-life hand gets near VR objects. But there's something to be said about lifting your empty hands in the VR sky and seeing your real fingers wiggle, which, based on pre-release tests, we can confirm Oculus Quest hand tracking nails.*
>
> *We've seen hand-tracking experiments on other VR headsets, but these have largely come in the form of proprietary add-ons like Leap Motion, which require additional hardware and a bolted-on rendering pipeline. These systems have been impressive enough as tested at various tech expos, but VR hand tracking has always been underwhelming in execution—just imprecise enough, in terms of recognizing individual fingers and "pinch" gestures, compared to the "it just works" appeal of a compatible controller.*

Magic Leap is pitching its old headset to businesses with a new name. The Magic Leap One Creator Edition, which shipped last August, is being replaced with the Magic Leap 1, which sells for the same price of $2,295. Good luck with that. (Adi Robertson / *The Verge*)

A blockchain firm called Saga, advised by Nobel laureate Myron Scholes, just launched a rival to **Facebook's Libra.** Both tokens are tied to baskets of currencies in order to stabilize their value. (Ryan Browne / CNBC)

Facebook's Portal just got some new features, including the ability to log in with a **WhatsApp** account.

The Verge made a list of the 100 gadgets that defined the last

decade, from the selfie stick in 2014 to Snap Spectacles in 2016. It’s fun!

And finally…

The holidays are upon us, and that means it’s time to take a look at the amusing ways that social networks are absolutely tearing us apart. Take it away, Julie Jargon:

> *The Laurendine-Scanlan feud has been particularly long-running, continuing to this day. And with the 2020 election nearing, it isn’t clear if it will ever end, despite each side’s wishes to put it behind them.*
>
> *“The last time I saw my dad’s entire side of the family was in 2015 — multiple aunts and probably 20-some cousins,” said Travis Laurendine, Lisa’s son, who hasn’t taken sides and wishes they could reconcile. “There have been no real efforts at reconciliation between my mom and aunt. Hopefully I can start to bridge the gap.”*

Fingers crossed.

Talk to us

Send us tips, comments, questions, and encrypted messages: casey@theverge.com and zoe@theverge.com.

https://www.theverge.com/interface/2019/12/11/21004135/encrypted-messaging-facebook-hearing-senate-whatsapp-messenger