

The Biden Administration Wants to Partner with Criminals to Spy on You

“The Biden administration,” CNN reports, “is considering using outside firms to track extremist chatter by Americans online.”

Federal law enforcement agencies are legally and constitutionally forbidden to monitor the private activities of citizens without first getting warrants based on probable cause to believe those citizens have committed, or are committing, crimes. The feds can browse public social media posts and so forth, but secretly trawling private groups and hacking encrypted chats is off-limits.

Private companies and nonprofit civic organizations, not being government entities, don’t need warrants or probable cause to access those private discussion areas. The administration’s bright idea is that through partnership with these non-government entities, they can get around legal and constitutional barriers: “WE didn’t collect the information. THEY collected the information, then gave it to us.”

There are several flies in that ointment. Here’s a big one:

It’s entirely understandable that — to use an entirely hypothetical example — someone with the Southern Poverty Law Center might impersonate a fictional white supremacist to get into a private Ku Klux Klan chat room and see what those people are up to.

But the US Department of Justice says it’s illegal (under the Computer Fraud and Abuse Act) to evade terms of service with false identities.

A government partnership with an organization that gathers information in that way is no different than the government partnering with a burglar to find out what you have in your house, without the bother of convincing a judge there’s probable cause to issue a search warrant. It is, quite simply, criminal conspiracy.

As with so many political and social issues arising in the Internet age, we’re coming up against a big question that urgently needs answering:

At what point does “working with” government amount to “being part of” government?

Much of the “private” tech sector makes big money on government contracts. NBC News reports, based on a 2020 Tech Inquiry expose, that Microsoft enjoys thousands of subcontracts with the US Department of Defense and federal law enforcement. Amazon has more than 350 such subcontracts with agencies like ICE and the FBI. Google, more than 250.

What about the “nonprofit” sector? According to the National Council of NonProfits, 31.8% of nonprofit revenues are tied to government grants and contracts.

When these entities do things FOR government, they should be held to the same standards and limits AS government. And those standards and limits should put our freedom and privacy first.