Don’t Wait: Get Into the Encryption Habit Now

In early August, a Nebraska prosecutor charged a mother and daughter with violating the state’s ban on abortion after 20 weeks. That ban was passed in 2010, but didn’t go into effect until the Supreme Court’s ruling earlier this year overturning *Roe V. Wade.*

Part of the state’s evidence consists of Facebook messages between the two, indicating that the mother obtained “abortion pills” for her pregnant daughter.

Police obtained those messages in the usual way: They presented a search warrant to Facebook and the company turned over the data.

If the two women had used Facebook’s optional “end-to-end encryption,” the police would still have been able to get that data — but they wouldn’t have been able to read it.

Facebook has since announced its intention to make end-to-end encryption the default, rather than an option, in its Messenger service.

That’s a good thing.

Whatever your opinion of abortion in general, or of Nebraska’s laws and the women’s alleged actions in particular, the case illustrates how easy it’s become for government to eavesdrop on our communications in real time, or seize and read our private files after the fact.

Between constantly advancing technical means, the tendency of judges to defer to law enforcement, and government’s willingness to just plain break the law when the law doesn’t suit their purposes (see Edward Snowden’s disclosure of the NSA’s illegal spying programs for examples), it’s become far TOO easy.

Some politicians on both sides of the major party aisle disagree. They don’t think it’s easy enough. They’re constantly working on laws they hope will make strong encryption less available (or, with “back door” schemes, just less strong).

This is the kind of battle that’s easier to fight now than later.

Strong encryption has been widely available for more than 30 years now.

But in order for the government to lose its war on our privacy, we need to see far more widespread adoption at both the individual and corporate levels … and we need that adoption to outpace unscrupulous politicians’ ability to keep up with it.

In a mostly unencrypted world, encrypted communications (of most kinds — there are exceptions) tend to stand out. In such an environment, it’s not unlikely that at some point, encryption will itself be deemed “suspicious” and its use treated as grounds for investigations and searches.

But if we’re all using encryption, all (or even most) of the time, prosecutors will need other pretexts, maybe even real evidence, to get permission to pry into our private affairs.

Which is exactly as it should be.

By using encryption on principle at least some of the time, and by asking your messaging providers to enable it by default, you’ll be protecting your privacy. And everyone else’s.