The Daily Dish

Tech Under Attack

DOUGLAS HOLTZ-EAKIN | MARCH 11, 2020

Eakinomics: Tech Under Attack

You might think that the coronavirus pandemic had ground all other policymaking to a halt. Not quite. Behind that drama there are a series of important discussions, including the future of freedom in tech settings. The focal point of the discussion is the Eliminating Abusive and Rampant Neglect of Interactive Technologies Act (EARN IT Act), which, in the words of its sponsors, would "create incentives for companies to 'earn' liability protection for violations of laws related to online child sexual abuse material." It's not quite that simple, as we shall see.

Mixed into the debate on liability issues is an attack on encryption technologies, led by Attorney General William Barr. As *The Wall Street Journal* reported,

> With a series of speeches, a sharply worded plea to Facebook Inc. Chief Executive Mark Zuckerberg and, now, a direct challenge to Apple Inc., Mr. Barr has intensified a long-running fight between law enforcement and technology companies over encrypted communications, potentially setting up a showdown with Silicon Valley. Some agents at the Federal Bureau of Investigation also worry his forceful approach could sour valuable relationships they have fostered with technology companies.
>
> Mr. Barr is disturbed not only by the potential harm that encryption technologies can cause law-enforcement investigations but also by what he sees as tech companies' ability to essentially defy court orders, people close to him said.

The law enforcement community's solution to encryption is to force tech companies to include "backdoors" that allow the authorities to bypass the encryption.

Now, as it turns out, platforms (e.g. Facebook, Yelp, or the comments section of your local paper) have a protection (Section 230 of the Communications Decency Act) from liability for user-generated content. Federal criminal activity, however, including much of the heinous content generating such concerns, is an exception to Section 230. So the EARN IT Act not only would create additional liability for things that companies largely are already liable for, but also could have consequences for legitimate content as well. And (shocking) sometimes the criminals use the same backdoor that is in principle labeled "Police Only." So this is an unholy mess of issues. Fortunately, AAF's Jennifer Huddleston has two roadmaps to the debates on Section 230 and encryption.

For me, the bottom line is pretty simple. In both cases, there is a desirable pursuit of bad guys, whether they be human traffickers or child predators or someone else. And in both cases there are better tools to use than attacking the current practices of the tech sector. This is true especially because we learned painfully after the attacks of 9/11 that you can too quickly trade freedom of communication (using encryption) for the pursuit of security. And the track record is that innovation is fostered by the liability protection of Section 230.

There *is* more going on than the coronavirus. In some cases, that's too bad.