

FORMER FBI ASSISTANT DIRECTOR MAKES A COMPELLING CASE TO ELIMINATE THE CORPORATION

Former FBI Assistant Director apparently isn't afraid to embarrass himself to fear monger for law enforcement.

That's the only conclusion I can reach by his penning this op-ed, which still bears its original title in the URL.

<http://www.washingtonpost.com/posteverything/wp/2014/09/23/i-helped-save-a-kidnapped-man-from-murder-with-apples-new-encryption-rules-we-never-wouldve-found-him/>

In it, Ronald T. Hosko claimed shamelessly that if Apple had been employing its new encryption plans earlier this year, a kidnap victim the FBI rescued would be dead. The two nut paragraphs originally read,

Last week, Apple and Android announced that their new operating systems [will be encrypted by default](#). That means the companies won't be able to unlock phones and iPads to reveal the photos, e-mails and recordings stored within.

It also means law enforcement officials won't be able to look at the range of data stored on the device, even with a court-approved warrant. Had this technology been used by the conspirators in our case, our victim would be dead. The perpetrators would likely be freely plotting their next revenge attack.

It made no sense! As Hosko correctly explained, they solved this case with lawful intercepts of phone content.

Once we identified potential conspirators, we quickly requested and secured the legal authority to intercept phone calls and text messages on multiple devices.

Even if the kidnappers had a new iPhone, FBI would still go to precisely the same source they did go to – the telecom providers – to get the intercepts. The FBI never even had the actual phones of kidnappers in hand – except for the phone the gang leader used to direct the plot from prison, which he crushed before it could be investigated, a technology that has been available to thugs far longer than encryption has.

So it is quite clear that, had this technology been used by the conspirators in this case, the FBI would still have caught them, using precisely the same process they did use to catch them..

After Hosko got called on his false claims on Twitter, he made two corrections – first to this interim fallback. (h/t @empirical error for catching this)

Had this technology been in place, we wouldn't have been able to quickly identify which phone lines to tap. That delay would have cost us our victim his life. The perpetrators would likely be freely plotting their next revenge attack.*

That didn't make any more sense, as they were tracing calls made from the kidnappers. Once they got close enough to examine their actual devices, they had the kidnappers. Now he has changed it to read:

Last week, Apple and Google announced that their new operating systems will be encrypted by default. Encrypting a phone doesn't make it any harder to tap, or "lawfully intercept" calls. But it does limit law enforcement's access to a data, contacts, photos and email stored on the phone itself.

That kind information can help law enforcement officials solve big cases quickly. For example, criminals sometimes avoid phone interception by communicating plans via Snapchat or video. Their phones contain contacts,

texts, and geo-tagged data that can help police track down accomplices. These new rules will make it impossible for us to access that information. They will create needless delays that could cost victims their lives.*

[snip]

** Editors note: This story incorrectly stated that Apple and Google's new encryption rules would have hindered law enforcement's ability to rescue the kidnap victim in Wake Forest, N.C. This is not the case. The piece has been corrected.*

Phew. Apparently all this surveillance technology is hard to keep straight, even for an experienced FBI guy. But the truly funny part of Hosko's piece – now that he at least has some semblance of factual accuracy (though I think he's still exaggerating about video and Snapchat) – is where he suggests that we should not avail ourselves of any technologies that make it easier on criminals.

If our cutting edge technologies are designed to keep important dots out of the hands of our government, we all might start thinking about how safe and secure we will be when the most tech-savvy, dedicated criminals exponentially increase their own success rates□.

This would lead you to believe Hosko is unaware of the "cutting edge technology" that has probably kept more crime-solving information out of the hands of the government than any measly encryption: incorporation. Drug cartels, human traffickers, even dreaded banksters all use shell corporations as a favored technology to not only hide the evidence of their crime, but to dodge accountability if it ever is discovered. That snazzy technology, the corporation, has empowered criminals far more

than cell phone encryption – with all the possible workarounds – will ever do.

Yet if you called for eliminating a beneficial technology like the corporation just because criminals also happen to find it useful, people would consider you batshit insane. It would be a totally disproportionate measure, trading away real benefits in the name of relative but not absolute safety.

But hey! Hosko has already embarrassed himself. So if he feels like doing so again, by all means, I implore him to call for the elimination of the corporation – or even just a few of the exotic financial tools that the most dangerous financial criminals use.

After all, it will make us safer!