CY VANCE CALLS IT IN DUMBLY ON SMART PHONES

There are two things Cy Vance (writing with Paris' Chief Prosecutor, the City of London Policy Commissioner, and Javier Zaragoza, Spain's High Court) doesn't mention in his op-ed calling for back doors in Apple and Google phones.

iPhone theft and bankster crime.

The former is a huge problem in NYC, with 8,465 iPhone thefts in 2013, which made up 18% of the grand larcenies in the city. The number came down 25% (and the crime started switching to Samsung products) last year, largely due to Apple's implementation of a Kill Switch, but that still leaves 6,000 thefts a year — as compared to the 74 iPhones Vance says NYPD wasn't able to access (he's silent about how many investigations, besides the 3 he describes, that actually thwarted; Vance ignores default cloud storage completely in his op-ed). The numbers will come down still further now that Apple has made the Kill Switch (like encryption) a default setting on the iPhone 6. But there are still a lot of thefts, which can not only result in a phone being wiped and resold, but also an identity stolen. Default encryption will protect against both kinds of crime. In other words, Vance just ignores how encryption can help to prevent a crime that has been rampant in NYC in recent years.

Bankster crime is an even bigger problem in NYC, with a number of the worlds most sophisticated Transnational Crime Organizations, doing trillions of dollars of damage, headquartered in the city. These TCOs are even rolling out their very own encrypted communication system, which Elizabeth Warren fears may eliminate the last means of holding them accountable for their crimes. But Vance — one of the prosecutors that

should be cracking down on this crime — not only doesn't mention their special encrypted communication system, but he doesn't mention their crimes at all.

There are other silences and blind spots in Vance's op-ed, too. The example he starts with — a murder in Evanston, not any of the signees' jurisdiction — describes two phones that couldn't be accessed. He remains silent about the other evidence available by other means, such as via the cloud. Moreover, he assumes the evidence *will* be in the smart phone, which may not be the case. Moreover, it's notable that Vance focuses on a black murder victim, because racial disparities in policing, not encryption, are often a better explanation for why murders of black men remain unsolved 2 months later. Given NYPD's own crummy record at investigating and solving the murders of black and Latino victims, you'd think Vance might worry more about having NYPD reassign its detectives accordingly than stripping the privacy of hundreds of thousands.

Then Vance goes on to describe how much smart phone data they're still getting.

> In France, smartphone data was vital to the swift investigation of the Charlie Hebdo terrorist attacks in January, and the deadly attack on a gas facility at Saint-Quentin-Fallavier, near Lyon, in June. And on a daily basis, our agencies rely on evidence lawfully retrieved from smartphones to fight sex crimes, child abuse, cybercrime, robberies or homicides.

Again, Vance is silent about whether this data is coming off the phone itself, or off the cloud. But it is better proof that investigators are still getting the data (perhaps via the cloud storage he doesn't want to talk about?), not that they're being thwarted.

Like Jim Comey, Vance claims to want to have a

discussion weighing the “marginal benefits of full-disk encryption and the need for local law enforcement to solve and prosecute crimes.” But his op-ed is so dishonest, so riven with obvious holes, it raises real questions about both his honesty and basic logic.