A GOOD REASON TO ENCRYPT YOUR IPHONE: TO PREVENT DEA FROM CREATING A FAKE FACEBOOK ACCOUNT

At Salon yesterday, I pushed back against the Apple hysteria again. In it, I look at the numbers that suggest far more Apple handsets are searched under the border exception than using warrants.

> Encrypting iPhones might have the biggest impact on law enforcement searches that don't involve warrants, contrary to law enforcement claims this is about warranted searches. As early as 2010, Customs and Border Patrol was searching around 4,600 devices a year and seizing up to 300 using what is called a "border exception." That is when CBP takes and searches devices from people it is questioning at the border. Just searching such devices does not even require probable cause (though seizing them requires some rationale). These searches increasingly involve smart phones like the iPhone.
>
> These numbers suggest border searches of iPhones may be as common as warranted searches of the devices. Apple provided account content to U.S. law enforcement 155 times last year. It responded to 3,431 device requests, but the "vast majority" of those device requests involved customers seeking help with a lost or stolen phone, not law enforcement trying to get contents off a cell phone (Consumer Reports estimates that 3.1 million Americans will have their smart phones stolen this year). Given that Apple has

> by far the largest share of the smart phone market in the U.S., a significant number of border device searches involving a smart phone will be an iPhone. Apple's default encryption will make it far harder for the government to do such searches without obtaining a warrant, which they often don't have evidence to get.

Almost 20% of Americans this year will have an iPhone, and that number will be far higher among those who fly internationally. If only 20% of 5,000 border searches involve iPhones, then there are clearly more border iPhone searches than warranted ones.

Meanwhile, we have an appalling new look at what law enforcement does once it gets inside your smart phone. A woman in Albany is suing DEA because — after she permitted DEA to conduct a consensual search of her phone — DEA then took photos obtained during the search, including one of her wearing only underwear, and made a fake Facebook page for her with them. They even sent a friend request to a fugitive and accepted other friend requests. They also posted pictures of her son and niece, on a site intended to lure those involved in the drug trade.

And they consider this a legitimate law enforcement activity!

> In a court filing, a U.S. attorney acknowledges that, unbeknownst to Arquiett, Sinnigen created the fake Facebook account, posed as her, posted photos, sent a friend request to a fugitive, accepted other friend requests, and used the account "for a legitimate law enforcement purpose."
>
> The government's response lays out an argument justifying Sinnigen's actions: "Defendants admit that Plaintiff did not give express permission for the use of photographs contained on her phone on an

> undercover Facebook page, but state the Plaintiff implicitly consented by granting access to the information stored in her cell phone and by consenting to the use of that information to aid in an ongoing criminal investigations [sic].”

To be sure, DEA and FBI would still be able to obtain consensual access to phones, as they did in this case, by threatening people with harsher charges if they don’t cooperate (which appears to be how they got her to cooperate).

But this demonstrates just how twisted is the government’s view of legitimate use of phone data. The next time you hear a top officer wail about pedophiles, you might ask whether they’re actually the one planning to post sexy pictures.