



DISTRICT ATTORNEY
COUNTY OF NEW YORK
ONE HOGAN PLACE
New York, N.Y. 10013
(212) 335-9000

CYRUS R. VANCE, JR.
DISTRICT ATTORNEY

February 5, 2016

Prof. Jonathan Zittrain, Faculty Chair
Berkman Center for Internet & Society at Harvard University
23 Everett Street, 2nd Floor
Cambridge, MA 02138

Re: *Don't Panic: Making Progress on the "Going Dark" Debate*

Dear Professor Zittrain:

In September 2014, Apple announced its decision to include default encryption of the password-protected content on its newest operating system, iOS 8. Google and others quickly followed suit. As a consequence, state and federal law enforcement agencies and national security agencies were faced with the fact that those who wished to avoid detection could communicate with one another so securely, that no governmental entity, even one armed with a search warrant issued by a judge, could access evidence on smartphones, including communications, contact names and numbers, photos, or videos. Such users would thus enjoy “full disk encryption.”

The response from law enforcement was swift. In particular, the Department of Justice and the Federal Bureau of Investigation warned that national security would be imperiled by full disk encryption. I also warned of the developments, arguing that they would compromise local law enforcement, as well as national security. My argument was set forth in a November 2015 report entitled “Report of the Manhattan District Attorney’s Office on Smartphone Encryption and Public Safety.”

The Berkman Center for Internet & Society at Harvard University has issued a report, dated February 1, 2016, entitled “Don’t Panic.” The Berkman Center’s report is largely a response to the concerns expressed by law enforcement (especially the FBI), and its message is aptly summarized by its title – according to Don’t Panic, although full disk encryption may make things harder for law enforcement in some circumstances, it is really not *that* big a deal.

I disagree. And, although I respect the care with which the authors of Don’t Panic have considered the problems posed by full disk encryption,¹ I think that the report misses some key points.

¹ As was made clear in the “Report of the Manhattan District Attorney’s Office on Smartphone Encryption and Public Safety,” neither I, nor any serious thinker about the problems discussed here, opposes all encryption. Encryption is essential because it serves numerous important goals. What I oppose is default “full disk encryption” on smartphones, which is impervious to governmental scrutiny even when such scrutiny is limited by the Fourth Amendment’s warrant requirement.

First, Don't Panic argues that widespread default encryption will never be very popular because "many companies' business models rely on access to user data." (Don't Panic at 10; *see also id.* at 10-12.) The argument seems to be that companies rely on user data to sell advertising and market research, and therefore the companies will not support robust full disk encryption because it would be against their own economic interests to do so.

The short (but sufficient) answer to that argument is that Apple, Google and other technology companies *have* supported full disk encryption because they believe there is a market for it that they wish to capture. Apple's announcement of iOS8 did not hide the fact that it offered full disk encryption, but trumpeted it: "Unlike our competitors, Apple cannot bypass your passcode and therefore cannot access [data on your smartphone if it is password protected]. So it's not technically feasible for us to respond to government warrants for the extraction of this data from devices in their possession running iOS 8."²

Second, Don't Panic notes that technology companies frequently have ongoing relationships with their customers. For example they do not simply sell a smartphone or an operating system to the customer, but they have data plans and storage agreements pursuant to which they store the customers' data in cloud storage. The report notes such relationships between technology companies and their customers would render robust encryption "impractical for companies who need to offer features in cloud services that require access to plaintext data." (Don't Panic at 11; *see generally id.* at pp. 11-12)

Once again, Don't Panic's argument is undermined by what Apple, Google and their followers have in fact done: The technology companies have told their customers – indeed, they have told the world – that the information on their smartphones will be unavailable to law enforcement, even if law enforcement uses lawful means (*i.e.*, a search warrant) to obtain that information. Either the companies are misleading the public, because the material is accessible, or they are entirely correct and the material is inaccessible, notwithstanding the cloud, back-ups, and data centers.³

Third, Don't Panic argues that the Internet of Things ("IoT"), in which "[a]ppliances and products" from televisions to toasters, to watches, bed sheets and toothbrushes are connected to the internet, is fast approaching and we will soon be so surrounded by sensors, microphones and detectors that, as a practical matter, all of those sources will be available to law enforcement and we will be in a state of near-constant surveillance. (Don't Panic at 10, 12-15) There will be no need to get into smartphones because we will have so much information from other sources.

My experience tells me that the IoT will not be as all-encompassing as Don't Panic suggests it will be. Even if evidence-collection through IoT can be done efficiently (I simply do not know if it will be as technically easy as Don't Panic seems to assume), people with something to hide can (and will) choose to avoid the IoT. And, smartphones contain information – including contact lists, photos, videos, and text messages -- that is often available nowhere else. The argument that law enforcement does

² Available on Apple's website, www.apple.com/privacy/government-information-requests/ (last visited, January 14, 2015).

³ Furthermore, as is noted on pages 6-8 of the Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety, even under the best of circumstances, *i.e.*, where the user backs up her or his smartphone to the cloud, the cloud does not keep large categories of data that are kept on the smartphone.

not need information from smartphones because it can obtain *other* evidence from IoT simply does not hold water.

Three signatories to Don't Panic wrote separate statements, which are included as appendices to Don't Panic. These, too, deserve brief comment.

Professor Susan Landau argues that encryption is necessary to protect intellectual property. True. But no one is arguing for an end to encryption *in toto*, only to an end to smartphone encryption that is impervious to government search pursuant to a warrant. That is, I am proposing reinstating the situation that prevailed prior to Apple's announcement in September 2014.

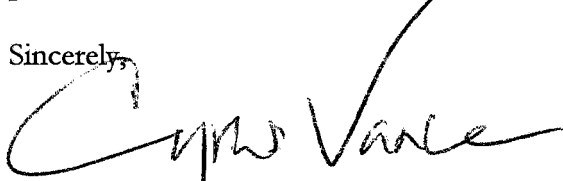
Bruce Schneier argues that full disk encryption is necessary to prevent hackers from compromising large amounts of data. The strength of this argument depends on whether full disk encryption prevents hacking, but I am not sure that is correct. In fact, I have repeatedly asked Apple and Google whether they could explain how their new operating systems made smartphones less vulnerable to hacking, and whether they had quantified how much safer the new operating systems rendered information on smartphones. Neither Apple nor Google has ever answered my questions.

In your individual statement, you warn against "burning the house to roast the pig," but I do not think that is at issue, at all. Barring full disk smartphone encryption is not burning the house, but helping law enforcement to protect its inhabitants from crimes and terrorist attacks. And, your observation that in "many . . . situations" the owner of the smartphone could "be ordered by a court to unlock the phone on pain of contempt," is simply wrong. The better view of the law is that a court cannot compel a person to reveal her or his password, or to use the password to unlock a smartphone in most cases. Moreover, the evidence sought may be in the phone of a victim or witness who is unavailable.

* * *

While no one is "panicking," there is reasonable cause for concern when companies that manufacture devices and operating systems that run 96.7% of the world's smartphones make them impenetrable to search warrants. Whether the companies should be able to do so is a matter for public discussion, and I applaud Don't Panic for advancing that discussion. As set forth above, however, I believe that Don't Panic does not adequately address the concerns of state and local law enforcement, who prosecute more than 95% of all crimes committed in the United States.

Sincerely,



Cyrus R. Vance, Jr.