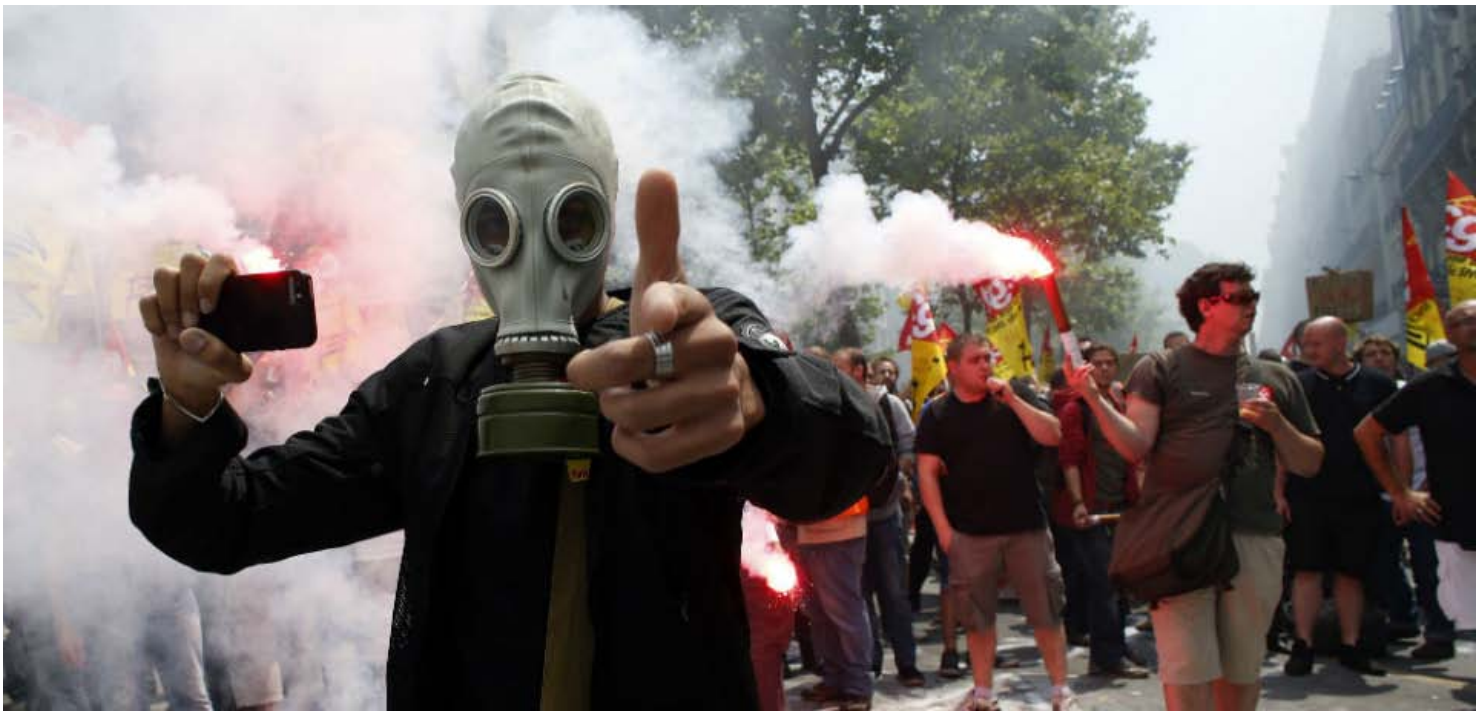
SHADOW GOVERNMENT Notes from the loyal opposition

Of iPhones, Backdoors, and Totalitarians

BY LINCOLN P. BLOOMFIELD, JR. FEBRUARY 23, 2016 - 1:39 PM



Having spent half my career as an appointed national security official in the past five Republican administrations, I appreciate and respect FBI Director James Comey and his organization. Having spent the other half in the private sector, including work with technology innovation companies, I also appreciate the role of Apple and other tech giants as a bright spot in America's underperforming economy. The standoff between the FBI and Apple over the former's demand for a backdoor to the iPhone pits two of the country's most important constituencies — the counter-terrorism community and the IT majors — against one other; and because each one's business is confidential, no bystander can fully assess the stakes on either side.

Yet, despite all the commentary backing the government's need to exploit available information about terrorist connections, and warnings — justified or not — about enabling government access to the sensitive personal data carried on password-protected smartphones, the debate has largely overlooked a third major

issue: the impact of either encrypted or exploitable cellphones on repressive regimes and the people trapped beneath them. While not the FBI's concern, it is a national security issue of real consequence.

About five years ago, an American general commanding troops in Afghanistan called an old friend, formerly with the government, to ask for help. His soldiers were texting each other during patrols to coordinate their locations, and the Taliban was picking up the transmissions with rudimentary electronic gear. Could the friend help? The result was an encryption program for cellphones that became commercially available by subscription. Programs were adapted to work with various models of cellphones, and designed for several geographies and languages, including Arabic. Subscriptions were provided gratis to opponents of the Assad regime in Syria, among others seeking political rights after the outbreak of the Arab spring.

The briefing I received on this technology made clear that programs like this would one day be readily available in every major market and language, eventually with layers of verbal "camouflage" over the encryption and an emergency feature for wiping a cellphone clean before it could be seized by authorities. One conclusion seemed inescapable: dictatorships around the world cannot stop the march of popular sovereignty enabled by information connectivity within their populations. Ruling regimes such as in China, Iran and Russia, who control broadcast media, censor social media and monitor communications, and who jail or execute dissidents to sustain themselves in power, cannot forever hold off the rising global tide of popular aspirations for basic rights.

Is there any doubt that a phone whose security code can be tried unlimited times by a powerful computer, with no delay or wiping of its content, would perfectly suit the internal security services of authoritarian

regimes? It is a question our national security community should be pondering at a time when popular discontent fueled by smartphone connectivity has brought masses into the streets, defying repression and corruption from Tunisia to Egypt, Syria, Iran, Ukraine, Hong Kong, and Malaysia.

Does this mean Apple should have its way and the FBI should be denied? Hopefully this does not have to be a zero-sum confrontation. A solution that did not compromise the security of current cellphone software would make it a little harder for undemocratic rivals of the United States to thrive, and a little easier for citizens seeking relief from oppression to find their voice and their courage.

News reports assume that U.S. authorities must be the ones to break into iPhones retrieved from terrorists like San Bernardino shooter Syed Farook. Has the government considered sharing its computerized code-breaking technology with Apple, and having industry recover the data from specific phones under court order? Apple's custody of this capability could be placed under the strict protocols of International Traffic in Arms Regulations defense trade controls, unable to be shared or exported except under State Department license.

Such a concept might have been unthinkable a few years ago — before the sensitive security records of more than 21 million people were hacked from the Office of Personnel Management, and before intelligence community contractor Edward Snowden fled to Hong Kong and Russia with a trove of classified information. The presumption that government know-how will be less secure in Apple's hands is no longer a given.

Hopefully a sensible, if unprecedented, compromise solution will be devised. When law enforcement authorities persuade a court that threats to public safety require access to information from specific captured iPhones, Apple should be provided the means to accommodate the public interest. If this can be accomplished for the sole benefit of U.S. counter-terror efforts, without Apple compromising the proprietary technology on its phones, not only will industry avoid harm to its brand and business, it will favor the interests of people everywhere rather than creating new tools for the world's totalitarians.

THOMAS SAMSON/AFP/Getty Images