WHAT MIX OF APPROACHES SHOULD WE USE TO KEEP CYBER SPACE SAFE?

President Obama gave a pretty crummy answer on Apple vs FBI at South by Southwest yesterday (I've put the entire exchange below the line). The question was posed as one pitting "privacy" versus security, and with the exception of this passage, Obama accepted that frame.

> What makes it even more complicated is the fact we also want really strong encryption, because part of us preventing terrorism, or preventing people from disrupting the financial system or our air traffic control system or a whole other set of systems that are increasingly digitalized is that hackers, state or non-state, can just get in there and mess them up.

Obama also bracketed two related issues: how our decisions will affect what happens in other countries, and how they'll affect our economic vitality (which is ultimately a cornerstone to America's hegemonic place in the world).

> And so the question now becomes, we as a society — setting aside the specific case between the FBI and Apple, setting aside the commercial interests, concerns about what could the Chinese government do with this even if we trusted the U.S. government — setting aside all those questions, we're going to have to make some decisions about how do we balance these respective risks.

Along the way he threw out some absurd examples, such as the security theater of TSA, or the claim that we need to break into smart phones

for tax enforcement when we still haven't shut down shell companies which are a bigger threat to tax enforcement, not to mention a tool used by big time criminals.

But underlying it all is an assumption, one shared by many of those taking the law enforcement side of this debate: that the police are the ones that keep us safe.

Don't get me wrong, what cops do *is* critical to keeping us safe, and there have definitely been times in my life I've been grateful to them (even if the time I was most victimized by crime, the cops also engaged in egregious racial profiling that made me angry).

But the cops are not the only thing that keeps us safe in this country — and our country relies on cops far more than many other countries and far more than we probably should. We probably rely on cops, in part, because we don't use armies to sustain domestic order, we have stark wealth differences (which are getting starker), and we also have used police to enforce racial caste in a way that few other countries expect their cops to do.

In addition to cops, however, we rely on other things to keep ourselves safe: common tools like door locks, operational security (after I got mugged I became far more aware of how and where I was walking at night), norms and civil society that serve as self-policing mechanisms, some alternative policing in privately owned public spaces. We do not ask cops to patrol inside our homes to keep burglars out (we do tolerate private guards, of a variety of types, patrolling commercial spaces, though they usually have far more limited authority), but rely instead primarily on other tools that work most of the time.

In meat space, I think the current state of affairs evolved over time (and again, is clearly a product of our economic and racial history); we're actually in a period of reassessment whether we've gotten the balance correct. But as

we debate how to keep law and order in “cyber” space, we seem to have forgotten that it takes more than police to keep us safe, even in meat space — and we certainly haven’t considered whether the same balance as we have settled on in meat space is appropriate in cyber space.

Meanwhile, the debate about law and order in cyber space takes place against the backdrop of national security in cyber space, with little clear differentiation between the two. It’s not an accident that those tasked primarily with national security are more supportive of real device encryption, partly for technical reasons, but partly because real device encryption negatively affects law enforcement far more than it negatively affects national security (and encryption definitely helps national security more than it hurts).

But one thing never happens in either of those worlds: accountability.

On the national security side, I have long noted that people like then Homeland Security Czar John Brennan or Director of National Security Keith Alexander never get held responsible when the US gets badly pawned. The Chinese were basically able to steal the better part of the F-35 program, yet we still don’t demand good cyber practices from defense contractors or question the approach the NSA used on cyber defense. A few people lost their job because of the OPM hack, but not the people who have a larger mandate for counterintelligence or cybersecurity. Indeed, the National Security Council apparently considers cyber a third category, in addition to public safety and national security.

As a result, whereas we assume (wrongly) that we should expect the NatSec establishment to prevent all terrorist attacks, no one thinks to hold our NatSec establishment responsible if China manages to steal databases of all our cleared personnel.

On the law enforcement side it’s not much

better: most cities have large numbers of crimes that never get cleared, including some of the crimes (like murder) that Jim Comey now says we can only solve if law enforcement can get inside your smart phone. And those uncleared crimes go back well before the time of smart phones. So the cops say they won't be able to solve crimes unless they can get inside your smart phone, but they're not, at the same time, being held accountable for the crimes they're not solving.

One thing is clear though: the OPM hack, not to mention the Target hack and the Sony hack and the Apple selfie hack, have made it clear that the government is not competent, by itself, to keep us safe in cyberspace. Even if it were true that we could or did rely exclusively on policing to keep us safe in meat space, the track record of "law enforcement" broadly defined may be even worse in cyber space. Or it may just be that the impact a few criminals can do is far more widespread (and also, far more likely to affect white victims).

One more thing: by merging Information Assurance Division with the rest of the NSA, the government recently made a decision to default to an even more offensive-minded posture on national security policing of the cyber world than it already had. I guess the idea is to aim for complete visibility in cyberspace and take out attackers that way. Maybe that's what needs to happen, maybe it's not. But the equivalent decision (even ignoring the privacy problems of OmniCISA) — expecting law enforcement to acquire total awareness of everything going on in cyber space — would be untenable in domestic cyber law enforcement.

I raise all this to point to a debate we're not having: one about what the proper means to keep cyber space safe is.

The assumption from people like President Obama is that ultimately self-defense, of which real encryption is a key part, must cede to police transparency. Yet that assumption comes with zero indication that that police transparency

will actually do much to keep cyber safe space.

I don't pretend to know the answer to what the proper model of public safety is. But I'm cognizant that we're assuming we know what it should be when in fact the evidence suggests that model is not keeping us safe.

Q A bunch of people wanted me to ask you about Apple and the situation with Apple and the FBI. (Applause.) You're trying to persuade the tech community that they should work with government. But it looks to the tech community – at least some in the tech community – that government is the enemy of the tech community in the way that it's dealing with Apple. Some in the tech community.

The question I want to ask you is, putting aside the specifics of this specific case, the legal fight between the company and the FBI, there are big questions around the idea of how you balance the need for law enforcement to conduct investigations and the needs of citizens to protect their privacy. This is the old privacy versus security debate. Mr. President, where do you come down on the privacy versus security debate?

THE PRESIDENT: Well, first of all, I can't comment on the specific case. So let's set that aside.

All of us value our privacy, and this is a society that is built on a Constitution and a Bill of Rights and a healthy skepticism about overreaching government power. Before smartphones were invented, and to this day, if there is probable cause to think that you have abducted a child, or that you are engaging in a terrorist plot, or you are guilty of some serious crime, law enforcement can appear before your – at your doorstep and say, we have a warrant to search your home, and they can go into your bedroom and into your bedroom doors and rifle through your underwear to see if

there’s any evidence of wrongdoing.

And we agree on that, because we recognize that just like all of our other rights – freedom of speech, freedom of religion, et cetera – that there are going to be some constraints that we impose in order to make sure that we are safe, secure and living in a civilized society.

Now, technology is evolving so rapidly that new questions are being asked. And I am of the view that there are very real reasons why we want to make sure that government cannot just willy-nilly get into everybody’s iPhones that is full of – or smartphones that are full of very personal information and very personal data. And let’s face it, the whole Snowden disclosure episode elevated people’s suspicions of this. So does popular culture, by the way, which makes it appear as if I’m in the Sit Room and I’m moving things – (laughter) –

Q You’ve been watching Homeland.

THE PRESIDENT: There’s like half a fingerprint and half an hour later, I’m tracking the guy in the streets of Istanbul. (Laughter.)

Q It’s not really that cool?

THE PRESIDENT: It turns out it doesn’t work that way. Sometimes I’m just trying to get a connection. (Laughter and applause.) But, look, that was a real issue. I will say, by the way, that – and I don’t want to go too far afield – but the Snowden issue vastly overstated the dangers to U.S. citizens in terms of spying, because the fact of the matter is, is that actually our intelligence agencies are pretty scrupulous about U.S. persons, people on U.S. soil. What those disclosures did identify were accesses overseas with respect to people who are not in this country.

A lot of those have been fixed. Don’t take my word for it. There was a panel that was constituted, an independent panel that just graded all the reforms that we set up to avoid those charges.

But I understand that that raised suspicions. All right. So we're concerned about privacy. We don't want government to be looking through everybody's phones, willy-nilly, without any kind of oversight or probable cause or a clear sense that it's targeted at somebody who might be a wrong-doer.

What makes it even more complicated is the fact we also want really strong encryption, because part of us preventing terrorism, or preventing people from disrupting the financial system or our air traffic control system or a whole other set of systems that are increasingly digitalized is that hackers, state or non-state, can just get in there and mess them up.

So we've got two values, both of which are important. Right?

Q Right.

THE PRESIDENT: And the question we now have to ask is, if technologically, it is possible to make an impenetrable device or system where the encryption is so strong that there's no key, there's no door at all, then how do we apprehend the child pornographer? How do we solve or disrupt a terrorist plot? What mechanisms do we have available to even do simple things like tax enforcement? Because, if, in fact, you can't crack that at all, government can't get in, then everybody is walking around with a Swiss bank account in their pocket – right? So there has to be some concession to the need to be able to get into that information somehow.

Now, what folks who are on the encryption side will argue is any key whatsoever, even if it starts off as just being directed at one device could end up being used on every device. That's just the nature of these systems. That is a technical question. I'm not a software engineer. It is, I think, technically true, but I think it can be overstated.

And so the question now becomes, we as a society – setting aside the specific case between the FBI and Apple, setting aside the commercial

interests, concerns about what could the Chinese government do with this even if we trusted the U.S. government – setting aside all those questions, we're going to have to make some decisions about how do we balance these respective risks.

And I've got a bunch of smart people sitting there, talking about it, thinking about it. We have engaged the tech community aggressively to help solve this problem. My conclusion so far is that you cannot take an absolutist view on this. So if your argument is strong encryption, no matter what, and we can and should, in fact, create black boxes, then that I think does not strike the kind of balance that we have lived with for 200, 300 years. And it's fetishizing our phones above every other value. And that can't be the right answer.

I suspect that the answer is going to come down to how do we create a system where the encryption is as strong as possible, the key is as secure as possible, it is accessible by the smallest number of people possible for a subset of issues that we agree are important. How we design that is not something that I have the expertise to do.

But I caution – I am way on the civil liberties side of this thing. Bill McRaven will tell you that I anguish a lot over the decisions we make in terms of how to keep this country safe, and I am not interested in overthrowing the values that have made us an exceptional and great nation simply for expediency. But the dangers are real. Maintaining law and order and a civilized society is important. Protecting our kids is important. And so I would just caution against taking an absolutist perspective on this.

Because we make compromises all the time. I haven't flown commercial in a while – (laughter) – but my understanding is it's not great fun –

Q It's not great. It's not great.

THE PRESIDENT: – going through security. But we

make the concession because – it's a big intrusion on our privacy, but we recognize it as important. We have stops for drunk drivers. It's an intrusion, but we think it's the right thing to do. And this notion that somehow our data is different and can be walled off from those other tradeoffs we make I believe is incorrect.

We do have to make sure, given the power of the Internet and how much our lives are digitalized, that it is narrow and it is constrained and that there's oversight. And I'm confident this is something that we can solve. But we're going to need the tech community – software designers, people who care deeply about this stuff – to help us solve it.

Because what will happen is if everybody goes to their respective corners and the tech community says, you know what, either we have strong, perfect encryption, or else it's Big Brother and an Orwellian world – what you'll find is that after something really bad happens, the politics of this will swing and it will become sloppy and rushed, and it will go through Congress in ways that have not been thought through. And then you really will have dangers to our civil liberties because we will have not done – the people who understand this best and who care most about privacy and civil liberties have sort of disengaged or taken a position that is not sustainable for the general public as a whole over time.