What If Snowden's Laptops Hold No Secrets?

The NSA leaker insists he'll never give classified data to the Russians. He may be telling the truth.

BY NOAH SHACHTMAN | JULY 18, 2013

In a letter to a former senator released this week, NSA leaker Edward Snowden swore that there is no way the Russian government can get any sensitive information from him -- despite the fact that he has been camped out in the Moscow airport for the past few weeks, carrying four laptops that he had supposedly used to lift the NSA's secrets.

"No intelligence service -- not even our own -- has the capacity to compromise the secrets I continue to protect," Snowden wrote to former Senator Gordon Humphrey of New Hampshire in an email published by the *Guardian*. "You may rest easy knowing [that] I cannot be coerced into revealing that information, even under torture."

At first glance, the message seems like more braggadocio from a man who has appeared to lay it on thick before, from his self-proclaimed ability to bug the president to his claims of being able to "**shut down the surveillance system in an afternoon**." It's widely assumed in both the business and the intelligence communities that any electronics brought into Moscow (or Hong Kong, for that matter) are going to be compromised by the country's spy agency. Perhaps he is underestimating the technical prowess of the Russian security services; perhaps he is overestimating his own.

But there's a third possibility: that Snowden is telling the truth. That there really is no way for him to give up any more information, other than the stuff in his head. Snowden may have left the United States with "**four computers** that enabled him to gain access to some of the U.S. government's most highly-classified secrets," as the *Guardian* put it. But he may not have those secrets now. The laptops could very well be empty -- and the secrets could be somewhere else.

Ever since Snowden's leaks began to appear in the press, Washington has been debating whether the former systems administrator is a whistleblower or some sort of spy. The latter position appeared to be radically strengthened when Snowden appeared in Hong Kong (where, presumably, the Chinese could get access to his laptops) and then in Moscow. Even if he didn't willfully cooperate with the governments there, they would drain his laptops of every last file. If those files were encrypted, that might slow things down -- but eventually, the secrets would be theirs.

The interpretation relies on Snowden, a veteran of a host of American intelligence agencies, being completely oblivious to Russia and China's well-known capacities to hack - or planning from the start to be an agent of a foreign power. Neither seems likely. Spies don't ask for asylum in a couple dozen countries**.** And former counterintelligence specialists -- even ones as young and unusual as Snowden -- aren't that out to lunch. As Snowden told Humphrey, "one of my specializations was to teach our people at DIA [Defense Intelligence Agency] how to keep such information from being compromised even in the highest threat counter-intelligence environments [like] China."

Of course, the best way to keep that information from being compromised is not to have it at all.

The closer you look at the "four laptops" story, the more it seems like a ruse designed to keep spies in Washington and Moscow guessing. Why would Snowden need four computers to carry the NSA data when a portable hard drive the size of a hand can carry terabytes of information? Why would he hold on to such information when he knew he would be a target for Western intelligence agencies -- entities that "no one can meaningfully oppose," as Snowden put it. "**If they want to get you, they'll get you in time**." Sure, the data could be a bargaining chip in a negotiation for political asylum. But what good is a bargaining chip, if it can be snatched from your hands?

The smarter play would be to give *someone else* that leverage -- to let one of Snowden's interlocutors, like Glenn Greenwald or Laura Poitras, hold on to the data. Or to split it up among a dozen different players. Snowden's team says they've already engineered a kind of digital dead man's switch, which can release a torrent of sensitive information in case the United States engages in "**extremely rogue behavior**," as Greenwald puts it. The metaphorical switch is designed to be flipped in Snowden's absence, not his presence.

In a sane world, the contents of Snowden's laptops would have legal ramifications. It's a more serious violation of the **Espionage Act** to deliver classified information into the hands of a foreign power than it is to simply make off with secrets that could be used to hurt the U.S. (One is punishable by death, the other by 10 years in prison.) But this world isn't always sane. On Thursday, a military judge allowed Wikileaker Bradley Manning to be charged with "**aiding the enemy**," since Osama bin Laden might have read one of the documents he disclosed on a news site. Whatever is on Snowden's computers, he's likely to face harsh punishment if he ever returns to the United States.

But there could be consequences in the way Snowden -- and future leakers -- are perceived, depending on whether his laptops are empty or full. Past **U.S. government whistleblowers** have already worried publicly that Snowden could damage the cause of tomorrow's crop -- allowing them to be branded them as traitors because Snowden supposedly put American secrets in Vladimir Putin's hands. What if he had no more secrets to digitally spill?

GUARDIAN/GLENN GREENWALD/LAURA POITRAS

Noah Shachtman is ***Foreign Policy's*** *Executive Editor for News.*

188 COMMENTS

Powered by livefyre

SIGN IN WITH TWITTER FACEBOOK LIVEFYRE

+ Follow conversation

POST TO □ TWITTER □ FACEBOOK POST COMMENT AS

Sort: Newest | Oldest

Conversation on FP.com

TerrenceKelleman
WARNING: This is pathetically supportive article of surveillance and should be ignored by anyone who cares for the true values of American democracy. This is counter intelligence at it's best/worst!

15 HOURS AGO

Like Reply

mhenriday
TerrenceKelleman FranzLiebkind But what, Terrence, do you expect from the pen/keyboard of Noah Shachtman - a reasoned discussion of the grave issues raised by Mr Snowden's revelations and those of other whistleblowers like Russell Tice (http://www.youtube.com/watch?feature=player_embedded&v=g1Lurd5QvZA) before him ? Fat chance - to paraphrase Gertrude Stein, «a shil is a shill is a shill». How else does one get to be «Executive Editor for News» of an organ like FP ?...

Henri

6 HOURS AGO

Like Reply

KaparaK
@Beedle, If am a "bigger traitor" for willing to trade-off part of my right to privacy to secure America by catching the Terrorists that caused the loss of thousands of innocent American lives in 9/11 and have continue their nefarous acts ever since, so be it, that is your warped opinion. At least, I don't have anything to hide, and perhaps you are collaborating with the likes of Benedict Arnold Snowden to sell your country to the enemy. Besides, in today's high tech age, do you really believe in privacy? If you do, then get off the Internet. However, if you rat to the enemy like Snowden and his ilks, be prepared to face the music. I am sure the Russians and Chinese would do likewise given similar circumstance which explain why they wanted to wash their hands off and rather have their senseless 3rd world goons in Venezuela & Columbia get ther hands dirty in the Snowden's sewer.

2 DAYS AGO

Like Reply

mhenriday
KaparaK beedle FranzLiebkind firefox0077 Well, «KaparaK», whether you are a traitor or rather a noble warrior against «terrorism» is a moot point, on which opinions, obviously, may differ. One thing is certain, however, the phrase is «and his ilk», without the superfluous «s». Perhaps before using words like «ilk», «nefarious», and «warped», or phrases like «get ther [sic !] hands dirty» you would be advised to study a little English semantics, orthography, and grammar....

Henri

2 DAYS AGO

Like Reply

KaparaK

mhenriday beedle FranzLiebkind firefox0077

"English" Professor mhenriday, pardon me for my grammar, however, I can bet you that I speak better "english grammar" thar the Queen of you know what. What matters to me most is the fact that you concur (at least, didn't disagree) with my opinion of Benedict Arnold Snowden and his traitorous "ilk" perhaps including you.

2 DAYS AGO

Like Reply

mhenriday

KaparaK beedle FranzLiebkind firefox0077 Sorry, KaparaK, but it has now become evident that not only is your knowledge of English semantics, orthography, and grammar defective, but also your reading comprehension in that language. I do not concur with your opinion of Mr Snowden - whose given names, by the way, seem to be «Edward Joseph», something which strangely enough seems to have escape so diligent an observer of the events in question as yourself - rather, I regard him as a hero, who sacrificed himself to bring government crimes to the attention of the public. Not being a US citizen, I can hardly be a «traitor» to the government of that country - but on the other hand, members of the US Congress have referred to Julian Paul Assange, who is an Australian citizen, by that term, so a misuse of the term on your part would hardly surprise me....

Henri

2 DAYS AGO

Like Reply

spat84

Retard! The damage is already done. The Russian some of the worlds most skillful cyber operators. What makes him think he can stop them.

2 DAYS AGO

Like Reply

mhenriday

spat84 FranzLiebkind @«Retard !», Now, now, «spat84» - it may be true that confession is good for the soul, but a comment thread on FP is hardly the place for self-castigation....

Henri

2 DAYS AGO

Like Reply

JK Seattle

I'm thinking encrypted torrent spread across computers of a selected list of NSA/CIA operatives with a mix of RF distributed across clouds in a variety of satellites that only need a torrent set of keys to open them. Skip RSS bit-wide encryption when you have RF options.

3 DAYS AGO

Like Reply

firefox0077

It doesn't matter what Snowden thinks about giving/not giving his laptop's data. It can be retrieved in 5 seconds with a thumb drive, unless he never sleeps, & takes his computer into the shower with himself...

4 DAYS AGO

Like Reply

Vurdyeidruks

What Edward Snowden has done, if there is any information to protect on those laptops, is protect the information at rest. You can't copy a hard disk to a thumb drive in 5 seconds, and even if you could, now you have 100 gigs of ciphertext to sit on, encrypted by a man who has state-of-the-art intelligence on Russian cryptanalytic capabilities.

4 DAYS AGO

Like Reply

schneibster

Vurdyeidruks I wish I was so old I couldn't understand what Snowden's done.

OTOH he's been a young fool. Hate to say it but there it is.

4 DAYS AGO

Like Reply

Cortland Richmond

schneibster Vurdyeidruks

Don't know if he has been a fool, precisely, but he has done something that is either foolish, necessary for our national well being, or damaging to our national interests; possibly all of that.

He may rightly rot in prison. What may we rightly do?

3 DAYS AGO

Like Reply

schneibster

Cortland Richmond Vurdyeidruks It wasn't necessary to our national well being; anybody with a brain knew al he "revealed" years if not decades ago.

Had he actually revealed skulduggery, like tapping the conversations of US persons overseas due to lack of due diligence in determining whether they were protected persons or not, or misuse of business communications that had been tapped for political or financial gain, I'd be yelling for heads to roll.

But he didn't find or report anything like that.

He wasted his life for nothing, for a "might have been." They mighta/coulda/woulda have violated our rights. That makes him a fool.

3 DAYS AGO

Like Reply

schneibster

firefox0077 Depends what he's done. If he merely kept them because they had incriminating material so he could wipe them clean, he's already done it, probably reformatted them and reinstalled operating systems, and has four laptops to keep himself occupied with while he waits to find out what's gonna happen and eats hot dogs (or whatever the Russian equivalent is- maybe piroshki which might not be too bad if you knew for sure what kind of meat).

4 DAYS AGO

Like Reply

schneibster

firefox0077 Hope he brought vitamins.

4 DAYS AGO

Like Reply

JCDavis

Snowden said before that he stashed the files all over the internet, and he's given Greenwald everything he's going to give him--Greenwald said the leak was over--so it's unlikely that Snowden has much of anything on him.

4 DAYS AGO

Like Reply

Vurdyeidruks

" If those files were encrypted, that might slow things down -- but eventually, the secrets would be theirs."

You mean, after the sun burns out?

4 DAYS AGO

Like Reply

firefox0077

Vurdyeidruks

Go get a computer education.

4 DAYS AGO

Like Reply

Vurdyeidruks

@firefox0077 I guess my education in CND from DOD and NSA didn't teach me about the functioning ultra-wide quantum cryptanalytic machines they will be deploying soon. Care to cite a source that indicates such a thing will exist prior to a functioning fusion reactor?

4 DAYS AGO Like Reply

mhenriday

Vurdyeidruks firefox0077 But Vurdjyeidruks, think about all those «fusion centres» in the US - surely they must be doing other things there than inspecting what sort of pornography their neighbours prefer ? No need to worry about the sun exhausting hydrogen supplies at its core in 4-5 thousand million years or the heat death of the universe in 10^100 years or so ; quantum-cracking is just 'round the corner !... ;-)

Henri

4 DAYS AGO Like Reply

Vurdyeidruks

@mhenriday maybe for d-wave and NSA, but not Russia. Maybe you have recent information to the contrary?

4 DAYS AGO Like Reply

mhenriday

Vurdyeidruks mhenriday I'd never underestimate the Russians, but no, I have no information to the contrary. My comment was meant ironically....

Henri

4 DAYS AGO Like Reply

FranzLiebkind

Vurdyeidruks firefox0077

Just a hunch--quantum computing sufficient for NSA's niche purposes will be available well before a practical fusion power reactor. (I have no direct experience here.).Ten exa-op supercomputers should be available around 2020, assuming that they can be cooled and afforded. (I have a fair amount of experience here, though cannot say for sure off the top whether they will be able to brute-force crack >256-bit RSA. No way on 2K.)

But isn't the easiest path to suborn the rather few certificate authorities?

4 DAYS AGO Like Reply

schneibster

FranzLiebkind Vurdyeidruks firefox0077 Actually what you do is buy a hundred dollar reverse-bias transistor shot noise random number generator and make your own CA. OpenSSL will let you do exactly that and the random number source manufacturers have OpenSSL modules and Linux device drivers.

Nobody has a non-quantum algorithm for breaking even large-prime encryption; and there is no quantum algorithm for breaking elliptical curve encryption.

4 DAYS AGO Like Reply

schneibster

FranzLiebkind Vurdyeidruks firefox0077 I can set one up and have you up and running generating 4096-bit certificates in about an hour once you have the hardware.

I have heard there are elliptical curve modules available; I haven't looked into it myself. If there aren't it's not that hard to code one up; say a month or so. You'll still need the random number generator.

4 DAYS AGO Like Reply

schneibster

FranzLiebkind Vurdyeidruks firefox0077 Here's one: http://discovery.csc.ncsu.edu/software/TinyECC/

Runs on an 8-bit processor; ideal for your cellphone.

4 DAYS AGO Like Reply

schneibster

FranzLiebkind Vurdyeidruks firefox0077 Here's a Java implementation, JECC: http://sourceforge.net/projects/jecc/

4 DAYS AGO

Like Reply

schneibster

FranzLiebkind Vurdyeidruks firefox0077 Oh, and BTW someone is making plug-in hardware ECC modules for one of the Cisco backplanes. 6200-series? Derp, don't ask me I'm not a network engineer. I can puzzle out how the stuff works.

4 DAYS AGO

Like Reply

Vurdyeidruks

1) Certificates have nothing to do with breaking at-rest encryption designed to be used by an individual. 2) NSA's needs and capabilities are irrelevant to the issue at hand, namely Russian capabilities. 3) Snowden has insider information on extremely sensitive domestic anti-terror programs, so I think it is not reasonable to assume that he doesn't have the same intelligence regarding the broad strokes of NSA cryptanalysis capabilities and subsequently utilized an encryption system which guaranteed the safety of the data, such as a OTP that he does not have the keymat for anymore. 4) His statements regarding the impossibility of revealing the key, even under duress, suggest that he has done exactly that. If he has, it is unbreakable, period. 5) Is it really reasonable to assume that NSA does not have control of the CA's? It could have just been good OPSEC that they didn't utilize such a capability against Iran.

4 DAYS AGO

Like Reply

FranzLiebkind

Vurdyeidruks

1. I wasn't referring to in-situ generation to be used by an individual--just a a general method by NSA to avoid brute force cryptanalysis and monitoring of unfortunately-named "backdoors" on hundreds of OS and browser, etc. variants--though there would be a complication if Snowden had to transmit a key to confederates.

2. I think it possible that China and Russia have suborned the authorities , though not likely. Sins of the flesh and all that

3 I would have expected his keymat to be useless in days.

4. Mostly agreed, except for caveat #1.

5. I am pretty confident that the NSA has control of CAs. I think they would be a helluva target for Russia, China, France, above all Israel. Such forbearance would be good opsec.

4 DAYS AGO

Like Reply

FranzLiebkind

schneibster Vurdyeidruks firefox0077

Ahh, like the thermal-noise generated random.org--which has given me anecdotally fishy result, though only when asked for number within a very small range.

4 DAYS AGO

Like Reply

FranzLiebkind

schneibster Vurdyeidruks firefox0077

I'm deferring more of my derp until I finish my systems design (with a couple collaborators) for a general NSA archival of most Internet payload. He wishes an article submittal; I am hella cautious.

If you have a current Oracle/STK price list that would be helpful.

4 DAYS AGO

Like Reply

Vurdyeidruks

FranzLiebkind Snowden has wikileaks support in addition to his own insider info as to NSA and SVR caps, I think the possibility that he hasn't properly circumvented their collection and analytic caps is remote.

Do they really use tape? I thought their storage was solid state custom stuff?

4 DAYS AGO

Like Reply

schneibster

Vurdyeidruks 1. Certificate based encryption is widely implemented in a number of convenient protocols, from browsers to email clients to encrypted voice and video feeds in appropriate clients and servers, and all of this is available in the public domain. No one but an idiot would waste time reinventing the wheel. Nothing prevents using a 4096-bit key in a standard CA for private use, issuing certificates and then revoking them regularly to improve security, setting up a network for private use. At this time this is as secure as anything; the closest anyone has come to breaking 4096-bit RSA is Eratosthenes' Sieve, and the implementation is not tractable in less than polynomial time.

From your reiteration of the misunderstanding about a CA, you're apparently not aware that the actual software to implement i is no big deal. It's keeping it secure that's the big deal. But of course, anyone idiotic enough to use a commercial CA organization for their secure network is either a major financial institution that has sufficient power to punish any national government that misuses its ability to break encryption, or Boris and Natasha, complete with bomb in safe and safe dropped on moose and squirrel.

Any competent software engineer can set up a CA on a single laptop or desktop computer of ordinary power- not even necessarily multi-CPU- in a day or less. I can do it in an hour because I'm used to setting up CAs to test edge cases in SSL software so I can fix bugs. I know how to diddle a CA to get a known sequence at the end of the root certificate. I had to do that to fix a pathological key case once upon a time.

The simple obvious solution is to set up a private CA. This allows you to control the entire cryptography feed cycle.

2. I'm talking about NSA's decryption facilities, which are actually also relevant to the topic under discussion. I use them as an exemplar because they are almost certainly the premier forced decryption organization on the planet. If they can't I submit no one can.

3. 384-bit ECC is accepted by the NSA for the encryption of data up to and including "Top Secret." I would expect codeword operations might stick with one-time-pads, which are clumsier but far more secure. What's to compromise? The keys? He had no access to keys for any codename operations.

All we found out is that the NSA watches incoming and outgoing connections across the US' international links. We already knew that. That the NSA could probably play network architecture games like Franz suggests and get mostly everything on the 'Net except China-to-China and Russia-to-Russia etc. completely non-US traffic. Which we also already knew. And that they don't do that to US persons (Note! Not just citizens!) without a warrant.

Sorry rest of the world, we keep an eye on what goes in and out, just like on ships and planes and trains and cars. If you don' like it you don't have to come in or go out.

4 DAYS AGO

Like Reply

schneibster

Vurdyeidruks 4. Agree; I'd break it into chunks and give it to my friends. If he's smart, it takes three of them together to reveal the entire key. It's not hard to work out how to do that.

5. Actually Iran broke into a western CA (European IIRC, I don't remember the country) and stole some root certs that gave them access to a bunch of emails Iranians outside the country were exchanging with activists inside.

But as I said, if you've got your own CA then it's as secure as you keep it.

4 DAYS AGO

Like Reply

schneibster

FranzLiebkind Vurdyeidruks 1. This isn't your area of expertise. They are called "public key encryption algorithms" for a reason. The encryption key does not help you to find the decryption key. Both ECC and RSA are public key schemes, using different underlying mathematical algorithms.

I can go into detail; you know enough math that you'll probably be fascinated. Just say the word. This is one of my specialties.

2. Doesn't matter for espionage. Nobody but an idiot uses anything but a private CA.

3. Agreed, but see my caveats to Vurdyeidruks on this point.

4. We all agree, but the caveat does not apply to a private CA.

5. In addition I'm pretty confident that the NSA serves as the repository for root CAs for most of the secure communications o the US, and it may also be available for the Department of Commerce to consult when it has questions (relayed from US firms) about data security or wants advice on adoption of commercial encryption standards.

4 DAYS AGO Like Reply

Vurdyeidruks

schneibster 1) Why are you still talking about certs in a conversation regarding the threat to data, at rest, that Snowden may have in his possession. Do you understand that is irrelevant to this question, and that Edward Snowden (along with WL support), with up-to-date intelligence on NSA and SVR/PLA(jk) caps cannot be reasonably assumed to have not mitigated these threats?

3) We're talking about how snowden has protected his information, again I don't understand why you bring up USG IA policies Irrelevant.

What we found out is that the previously non-authorized collection program has been authorized and upgraded, and is specifically targeted domestically. I agree that nothing that Snowden revealed should surprise anyone with healthy suspicion and any knowledge of past NSA activities. The issue is that it continues to occur, and is legislatively authorized.

The NSA does collect all this data on US persons. They just claim they don't inspect it until authorized. For some reason, people have a problem with that. Perhaps due to the USG's sordid history regarding domestic COINTEL programs, classifying merely embarrassing or criminal information, and recent nose-dive in the realm of transparency.

4 DAYS AGO Like Reply

schneibster

FranzLiebkind Vurdyeidruks firefox0077 One of the things you have to make sure of is the temperature of your source. The good ones have a Peltier device and a thermostat and a heating coil, and start posting errors when the heater or cooler goes out (1,000,000 hours according to the data sheet, IIRC). Temperature variations can introduce systematic errors that weaken the randomness.

4 DAYS AGO Like Reply

schneibster

FranzLiebkind Vurdyeidruks firefox0077 Me not salesman. Me engineer.

4 DAYS AGO Like Reply

schneibster

Vurdyeidruks 1. I disagree. The easiest way is to use a private CA and then break the private key apart and distribute it. The details vary with the type of encryption.

You don't even appear to understand what a private CA is. Certainly you've never set one up or you would understand that it doesn't matter what commercial CAs have been compromised or by whom.

You can generate your own Root CA Certificate and create multiple CA installations/repositories with their own derivative root certificates FOR FREE. All you need is a computer and a $100 piece of hardware to generate random numbers. The operating system and the software are free. There's an excellent chance I still have a root CA on my Linux box upstairs and I can probably generate a root cert if you like.

3. What did he compromise? Please be detailed. Because nothing in either of Greenwald's articles was any surprise to me, and I sure don't work for the NSA. In fact I didn't hear anything I haven't known my entire career; learned it in school.

Greenwald even says, in both articles: the NSA gets nothing without a warrant but records of incoming and outgoing connections.

Snowjob has nothing; he thought he was selling out and it turns out he's a fool.

4 DAYS AGO Like Reply

schneibster

Vurdyeidruks Consider this: perhaps he kept the laptops with him so he could run 50x overwrite on their hard drives on the plane to Hong Kong.

That can take a long time.

4 DAYS AGO Like Reply

schneibster

FranzLiebkind Vurdyeidruks firefox0077 They're not going to lock you up for discovering mathematics (which systems engineering is a branch of) no matter how many times you've watched Sneakers.

4 DAYS AGO Like Reply

schneibster

FranzLiebkind Vurdyeidruks firefox0077 Oh, and I didn't mean to sound like I was lording it over you; having heard you speak about networking equipment you obviously know your shit, way more than me. I'll be interested to see your thoughts. This stuff is one of my professional areas of expertise. I have fixed many SSL bugs. I was the specialist in this area, and in the area of networking protocols and DNS.

And if you've never encountered the Diffie-Hellman algorithm before you will find it mathematically interesting.

4 DAYS AGO Like Reply

Vurdyeidruks

schneibster Have to re-write the firmware first for that to work, for obvious reasons. Don't you know we just burn everything now?

4 DAYS AGO Like Reply

schneibster

Vurdyeidruks Why are you making up stories about having to implement 50x overwrite in firmware? I know where to burn a boot CD that I can do it from. Knoppix.

4 DAYS AGO Like Reply

Vurdyeidruks

schneibster What you don't understand is how modern hard disks map the logical space to the physical. 50x overwrite isn't the issue. The issue is with even being able to wipe the entirety of the disk a single time.

4 DAYS AGO Like Reply

schneibster

Vurdyeidruks Actually my other specialty is filesystems.

Oops.

4 DAYS AGO Like Reply

Vurdyeidruks

schneibster This is a hardware issue specific to how the disk's operating system remaps the disk on-line to support reliability.

4 DAYS AGO Like Reply

schneibster

Vurdyeidruks That's why you use Knoppix. They've got diagnostic programs for all the disk types right there ready to run; in a dosbox if necessary.

4 DAYS AGO Like Reply

Show 50 More

FOLLOW US ON TWITTER | **VISIT US ON FACEBOOK** | **FOLLOW US ON RSS** | **SUBSCRIBE TO FOREIGN POLICY**

ABOUT FP | MEET THE STAFF | FOREIGN EDITIONS | REPRINT PERMISSIONS | ADVERTISING | WRITERS' GUIDELINES | PRESS ROOM | WORK AT FP

SERVICES:SUBSCRIPTION SERVICES | ACADEMIC PROGRAM | FP ARCHIVE | REPRINT PERMISSIONS | FP REPORTS AND MERCHANDISE | SPECIAL REPORTS | BUY BACK ISSUES

PRIVACY POLICY | DISCLAIMER | CONTACT US

FP Foreign Policy

11 DUPONT CIRCLE NW, SUITE 600 | WASHINGTON, DC 20036 | PHONE: 202-728-7300 | FAX: 202-728-7342
FOREIGN POLICY IS PUBLISHED BY THE FP GROUP, A DIVISION OF THE WASHINGTON POST COMPANY