THE BROOKINGS INSTITUTION

CYBERSECURITY AND CYBER FREEDOM:

THE FUTURE OF DIGITAL SURVEILLANCE TECHNOLOGY

Washington, D.C.

Monday, February 14, 2011

PARTICIPANTS:

Featured Speaker:

SUSAN LANDAU
Fellow, Radcliffe Institute for Advanced Study

Moderator:

ALLAN A. FRIEDMAN
Fellow, Governance Studies
The Brookings Institution

Panelists:

STEWART A. BAKER
Partner, Steptoe & Johnson LLP

SUSAN LANDAU
Fellow, Radcliffe Institute for Advanced Study

* * * * *

P R O C E E D I N G S

MR. FRIEDMAN: Good afternoon. And thank you for taking some time out of a lovely afternoon to spend some time inside talking about what I hope is going to be a very exciting topic.

So, usually, discussions of cybersecurity begin with, you know, someone pointing out that information technology has changed the world. I think we can all take these comments as read. You're all here with you agree with this. And let's focus on a fairly specific question, which is: the future of digital surveillance.

Now, this is a very timely question. On Thursday, we're going to be having hearings in the House Judiciary Committee. Congressman Sensenbrenner has titled the hearings, "Going Dark: Lawful Electronic Surveillance in the Face of Technologies." And elsewhere on the Hill, Congressman Mike Rogers has been talking about the need to revisit CALEA, the Communications Assistance for Law Enforcement Act, which we're going to hear a lot about today, saying that as long as it's consistent with due process, we're going to have to continue to expand surveillance. We know bad guys are communicating trough Facebook -- and online video games. And it's foolish for America not to keep pace with the changing world of online communication.

Now, on the flip side, we've all seen what happens when the wrong people pay attention to online communication. And Congressman Bill Keating has talked about how the Iranian and Egyptian protests have taught us that social media can be as powerful as any gun. And he's even cautioned us, saying that companies that are selling technology to countries using it to perpetuate human rights abuses mush work with Congress to make this right.

So this is a very current question, to say how are we going to think about what the government can and can't do for communication technology, in terms of protecting us from legitimate harms but, at the same time, respecting civil liberties -- and also other questions that we're going to be talking about today.

Now, fortunately, in the face of a very current topic, we have Susan Landau, who has just written a book titled *Surveillance or Security: The Risks Posed by the New Wiretapping Technologies*, which has just come out by MIT Press. Susan is spending the year at the Radcliffe Institute, Harvard-Radcliffe, but until 2010 was a staff engineer, and then a Distinguished Engineer at Sun Microsystems, where she worked not only on technology issues, but also a lot of policy issues, focusing on security, from surveillance digital rights management and, before that, cryptographic export control -- and has some fun stories about that battle.

Now, to balance the discussion, we have Stewart Baker, who comes to us from Steptoe & Johnson, but he was also the first Assistant Secretary at Department of Homeland security for Policy. And, before that, in 1990s, was General Counsel of the National Security Agency -- and has some incredible insights on what is actually going on, as well as some very unique and iconoclastic perspectives that will, I think, have a great discussion.

So now I'd like to invite Susan to talk about where she things these new technologies are going, and some of the risks that are going to be introduced. And then we'll have a panel discussion about sort of how do we measure these, how do we balance them, and then we'll take questions from the audience.

MS. LANDAU: Thank you very much, Allan.

So, Allan wants us to talk about the future. But you can't talk about the future until you think a little bit about the past. And I want to take you briefly back to 1992, when the U.S. government permitted the export of very strong cryptography -- 40 bits. For those of you technically inclined, you know, you can break it on your laptop in under a minute now. And, in fact, it didn't take very long to break in the mid-1990s.

The other thing that the U.S. government did in 1992 is that the FBI began pushing the passage of a bill called "Digital Telephony." The FBI was worried about going dark. It was worried that it couldn't

handle the new telephone technologies like call forwarding and other innovative technologies of the time, and it asked that all digitally-switched telephone communications be built wiretap-enabled, with the standards developed by the Federal government.

What happened in 1992 was not much. Industry was not happy by the U.S. government's concession, and Congress was not interested in the FBI's proposal. Nobody sponsored the bill.

Move forward two years. Now, at that time, the FBI claimed that by 1994, 1996, 40 or 60 percent of all phone communications would be encrypted. Except for those of you using Skype and government devices, I bet nobody every talks on an encrypted phone -- yet.

Move forward to 1994, when the FBI proposed its bill again, it changed the name to the Communications Assistance for Law Enforcement Act, and it threw in a sweetener to the telephone companies -- $500 million to help update their systems. And the telephone companies dropped their opposition. So the only people left opposing was industry -- the computer industry -- and the civil liberties groups. And the FBI said, "We don't need to have this bill apply to the internet. We only want it for phone communications."

What happened through the rest of the 1990s? Well, the U.S. government didn't want to see the export of devices with strong cryptography. And they didn't want to see the use domestically of devices

with strong cryptography. So the way to do this was prevent export, and then computer companies wouldn't build things domestically that they couldn't ship abroad, because half their market was abroad.

But other things happened, too. You guys know when you type in "www.Amazon.com" you go to Amazon. But your computer doesn't actually know where Amazon is on the network. It does a lookup to find what's called the IP address -- the internet protocol address -- of Amazon. Now, if you use Amazon enough, it might keep that stored relatively locally. But if you go somewhere new -- the Brookings Institution page, to the House Judiciary Committee page -- it has to look it up.

What ensures that when you try to go to Bank of America, you're going to Bank of America, and not something that looks like Bank of America? When you go down the street there's no real problem, because there's this red brick building with the ATM slot in it, and it would be really weird to have somebody build a red brick building with an ATM slot that says "Bank of America" that isn't, because you have to go through the whole permitting process, it takes a long time, it's an expensive process. And so you know, when it says "Bank of America" and it has the ATM slot right in the building, and there isn't something on top of the ATM slot that's spoofed -- you know, when you do that that you've got the real Bank of America building.

But when you go to the virtual world and you try to have that in the virtual world, how do you know? Well, it turns out it's a real problem. And the computer scientists, the technologists, have a solution that involves digitally signing a whole bunch of URLs to ensure that when you type in "Bank of America," you really get to Bank of America, and not some spoof.

We've had that system since the mid-1990s. But in the mid-1990s the U.S. government prevented the export of this protocol abroad, because it used cryptography. This was a very short-sighted plan.

Now the U.S. government is pushing that. So, in fact, it's been Federal policy for the last two years -- Office of Management and Budget has required, since 2009, that all Federal civilian agencies use what's called DNSSEC. And, in fact, the military is requiring that for all military agencies. But in the 1990s, the U.S. government went the other way.

So now I want to jump to now. And I want to jump to now in two different ways.

The first way is attribution. And all of you know the problem of you get something from the network and you don't know if it's really from the person you thought it was. You don't know if the thing is coming from where you expect it to be. You don't know if you're getting the right information. And if you're in the military, you care a lot about attribution

because, of course, you can't respond if you can't attribute it to the right place.

So in the network, we have what are called "layers." The application layer is what all of you know and love, and most of you think of as the "internet" -- Amazon, Facebook, Google.

If you go down further, in terms of how the network is actually architected, all of your messages -- whether you're talking an e-mail, whether you're talking about an instant message, whether you're talking about a web

page -- is broken up into little packets. And your message transits the network in funny little ways all across. And in Washington, there's been a lot of talk the last couple of years: we need attribution of those packets. We need to know that those packets really are where they say they're from.

But it turns out that the problem is actually a lot more subtle. There are a whole bunch of different crimes on the network. There's spam, which is problematic and annoying, and not a lot more. There's distributed denial of service attacks -- what brought down Estonia a few years ago. The attacks on the Republic of Georgia during the time of the Russian war with Georgia. There are criminal activities on the network.

And there's cyber exploitations where somebody, parties unknown, go into a machine a Northrop Grumman, or Lockheed Martin, or the Defense Intelligence Agency, and pull out material. And they do it very carefully and very well. They sit inside the machine for a long time looking at where the files of interest are. And when they decide to download them it happens all very quickly. It goes to a machine in Taiwan or a machine in Korea, and eventually seems to end up in Southern China. Where it goes from there, we know not.

And so the cry in Washington is, “We need to be able to attribute those attacks.” “We need the packets, the low-level pieces of information that transit the internet, to tell us where they’re coming from.”

So I looked at this problem with a colleague at MIT, and we began to think about what is the real problem? When you look at a DDOS attack -- when you look at a distributed denial of service attack -- what you’re interested in doing is stopping the attack. That’s the only thing you want to do. Sure, you’d like to get back at the guy who did it to you, but that’s much less important than stopping it.

And I don’t know how many of you watched what happened when Amazon pulled WikiLeaks. When Amazon pulled WikiLeaks it was the subject of a denial of service attack. But for Amazon, denial of service is kind of like Christmas. It’s when everybody comes to their machine to try and order books for the holidays. Amazon withstood the attack without a problem.

The fact is, you can architect to withstand the problem. And you can protect yourself against the problem.

For criminal activities, it’s really useful to know where the packets come from, because that’s the start of an investigation. And every law enforcement person will tell you that. But notice the word I used -- “start.” At the end of the investigation, you need to tie a real human

being to the criminal activity. That means you need to see who withdraws the money from the ATM machine, who takes that stolen credit card and buys things with it, and so on.

And so attaching identity to this low-level information is not that useful.

As for cyber exploitation, well let me stop a minute and tell you that two different techniques are used in criminal activities. The first one is a multi-step attack in which, for example, somebody downloads information about you from TJ Maxx, and then later takes that information to create a credit card -- in your name. That's multi-step -- the step of downloading the information, and then creating the fake credit card.

Multi-stage is something else. It's when that data is taken from the machine at Fort Huachuca and downloaded to a machine in Taiwan, and then downloaded to a machine in Korea, and then downloaded to a machine in China.

When it's downloaded to Taiwan, as long as we have a judicial relationship, a legal relationship with Taiwan, we can ask for the ability to examine the machine where the data went, to examine the ISP. And then we can find, "Oh, it went to Korea."

But as soon as it disappears into the dark neverland, where we don't have judicial, legal, connections, we can't do anything. We can't

find out -- did it stay in China? Did it go to Russia? Did it go somewhere else?

And so that begins to make it clear that the whole issue of cyber exploitation -- which is, by the way, the most serious cyber security problem we have. It's not cyber war, it's cyber exploitation.

William Lynn, the Deputy Secretary of Defense, wrote in *Foreign Affairs* last summer that the most serious long-term national security threat -- cybersecurity threat -- is cyber exploitation. That the amount of data being stolen -- intellectual property, business plans, patents, research ideas, and so on -- is so huge it swamps the Library of Congress each year.

So the problem there is not solved by technical means, it's solved by legal means. And it's a complicated one.

Now, as Allan mentioned, law enforcement is having some trouble wiretapping these days. There are all sorts of new communications technologies. Google came up with one a couple of weeks ago in Egypt, in which its newly-acquired SayNow was combined with Twitter and Google Speak-to-Voice, and it enabled the Egyptians to be able to get messages out even when the internet was down.

There are all types of new communications technologies, and they provide a real challenge to law enforcement. And that's true.

And so what law enforcement would like to do is change CALEA -- now, I say, "what law enforcement would like to do" -- I don't know what law enforcement would like to do. There are a series of *New York Times* and *Washington Post* articles that say "law enforcement would like" to do this, "law enforcement would like" to do that. They haven't been followed up with an Administration bill, yet. But the *New York Times* and *Washington Post* articles say, " -- expand CALEA to internet communications."

The problem with doing so is that internet communications are fragile. We wouldn't be having conversations about cybersecurity if we knew how to protect the internet. We wouldn't be having any of these conversations. If we had security on the network, this wouldn't be a problem.

The issue of CALEA on the internet -- CALEA involves building wiretapping capability into the fabric of the communication system. And when you do that, you've got what we call in the trade, an "architected security breach."

Let me tell you some examples of when these happen -- of when these have happened.

In Greece in 2004, 2005, a hundred senior members of the Greek Government, including the Prime Minister, the head of the Ministry

of Defense, of the Interior, and so on, were wiretapped for 10 months. The intruders broke into a switch in Vodaphone Greece network. The switch has wiretapping capabilities in it -- not because Vodaphone Greece wanted them. They hadn't paid for them, so they weren't supposed to be switched on. But Ericsson, who built the switch, had put it in to comply with European standards on wiretapping.

Because it wasn't purchased, the auditing capability wasn't part of the switch. Somebody went into the switch, turned on the wiretapping capability, and tapped a hundred members of the Greek government for 10 months.

I can tell you in great detail how it was done. I can't tell you who did it. It stopped when Vodaphone Greece discovered some SMS messages went awry, tried to figure out what happened. The wiretapping stopped, but we still don't know who did it.

Telecom Italia, for a period of 10 years -- 6,000 Italians, one out of 10,000 Italians -- 6,000 Italians were wiretapped. This included judges, business people, celebrities, sports figures. Think about it. Why would you wiretap those people? Blackmail and bribes. Insider attack.

When you build wiretapping capability that can be easily turned on, people from the outside can do it -- as in the Greek case -- and people from the inside can do it, as in -- apparently -- from the Telecom

Italia case. The case happened 1996 to 2006. It is still wending its way through the Italian courts.

Another example is that an IBM researcher, Tom Cross, discovered a year ago that a Cisco architecture for IP networks, for wiretapping IP networks, compliant with European standards can be spoofed. What that means is some bad guy, sitting inside law enforcement -- like a Robert Hanssen -- can go and look at whether or not he's being wiretapped and can shut off the auditing capability, so that nobody ever knows he looked at the system.

In fact, if we look at the FBI system for wiretapping IP networks -- Carnivore, later renamed DCS3000 -- it was also possible to spoof it, because it had very poor auditing capability.

So we need to think about what our serious risks are.

At the time we passed CALEA, we said the serious risks were organized crime, drug dealing, kidnapping -- although kidnapping was something of a red-herring, because it turns out that wiretaps are very rarely used in kidnapping cases. You don't know who the kidnaper is, so you can't tap their phone. And if you want to listen in to the family, that's not a wiretap, either legally or technically. So wiretaps are used only four or five times, maybe six times a year in the 450 wiretaps -- in the 450 kidnapping cases we have.

That was then. Now our risk is cyber exploitation. Now our national security risk is cyber exploitation. And the risks come from nation states on the outside, and sometimes from insiders, inside the company.

Fairchild Semiconductor lost thousands of pages of information to the Japanese Consulate in San Francisco, 20, 30 years ago -- lost enough information that it suffered a takeover attack from Fujitsu, and the U.S. government had to bail it out.

The other issue is that switches last a very long time. When you build a wiretapping capability into a switch now -- or you do it in 1994 or 1996 to comply with CALEA -- switches last a lot longer than you PDAs, your laptops, your cell phones. Those last two years, three years, at the outside. Switches used to last 40. They don't last quite as long.

But the point is that threat models change, and we're stuck with a surveillance technology that's looking at us.

So -- I've told you what law enforcement wants. Let me tell you a little it about what the NSA wants. And now I think that Stu and I will have some interesting tangling.

In the 1990s, the NSA fought very hard against allowing crypto to be exported -- products with strong cryptography. That also prevented the use of products with strong cryptography domestically, which made the FBI happy.

1999, the NSA changed its mind -- changed its mind for a number of reasons, including if U.S. industry didn't produce those products, somebody else was going to. And one of the things about the U.S. industry producing it is, NSA could sometimes get a look-see at the U.S. products ahead of time, and figure out how to go around the crypto. But they couldn't do that when stuff was made abroad.

But the other issue is that one of the important aspects of the NSA -- the part that never gets the publicity -- is the Information Assurance Directorate. It's only 15 percent of the budget, but it's 50 percent of the mission. Its job is to keep U.S. government material safe, U.S. government information safe.

But the NSA periodically dabbles in information elsewhere. When IBM was being wiretapped by the Russians in Glen Cove in the 1970s, they were communicating via a private network using microwave towers. NSA went to IBM and said, "You need to change this. You're in trouble, guys."

And so the NSA has had a very interesting response over the last 10 years. It has approved a public algorithm for use in top-secret communications. It has come up with a suite of algorithms that are NIST standards -- standards that came through the National Institutes of Standards and Technology, a civilian agency. It has approved those

standards for use in building a secure communications network. It has allowed soldiers in Iraq to buy commercial, off-the-shelf equipment for developing secure communications. Because when they were working in Iraq with Iraqi forces, they needed to be able to have systems put together quickly.

So the NSA interest has changed somewhat. The NSA is saying, “We’ve got to have this out in the public sector.” In fact, I was talking to somebody at the Information Assurance Directorate a year ago, and he was talking to me about first responders. First responders -- police, fire, ambulance -- use land mobile radio. They can’t use cell or internet, because that might go down in a crisis. They can’t use satellite, because sometimes clouds or mountains or tall buildings block them. So they use land mobile radio.

If you think about it, a police car has a gazillion different antennas. That’s because they need an antenna to communicate within their district. They need an antenna to communicate outside their district. They need an antenna to communicate with EMTs inside their district, outside their district. Fire, inside, outside -- that’s all the antennas they’ve got. Pretty stupid.

And what this man said -- the technical director from the Information Assurance division of NSA said -- he said, “I want to see

secure land mobile radio available in Radio Shack. Because then it's cheap and easy for all first responders to have."

But, of course, it's not only first responders who are going to buy secure land mobile radio. It's a lot of the bad guys, too.

Now, you could say, well, NSA doesn't have to worry about the bad guys on the inside. But people in the government do. Yet it is NSA policy, "Let's put secure communications out there."

So, as I look at the world we've got, what is it we need?

Well, I've told you a little bit about security. The events of the last three weeks also told you a little bit about security against the government. And so another thing that's gone out in the last 20 years is that U.S. diplomats are less in presence in certain places -- the last 10 years. And they often rely on NGOs, on oil companies. Oil companies know more about what's happening in parts of Indonesia than the U.S. government.

Those people need secure communications. So does law enforcement and national security need secure communications of a different sort. They sometimes need anonymized communications. Sometimes there are Navy personnel working in the Middle East, and they will need to communicate back with Annapolis. But nobody in the Middle East knows that they're Navy personnel. They're just guys. And so they

need a form of communication that hides who they're communicating with. And that type of communication -- the "onion routing" -- was developed at the Naval Research Labs -- to anonymize who the end-point of a communication are.

But it's not used just by the military and law enforcement, it's used more broadly. Because if it's just U.S. military and law enforcement who use it, then it's pretty easy to tell those guys in the Middle East are U.S. personnel. So the saying in the trade is, "anonymity loves company." And that product has been released for public use. You can go to the OnionRoutingTor.eff.org to find it.

So we have very interesting efforts on the side of the U.S. government -- pushing for anonymity and pushing for secure communications.

What we need to do, as we think about all these issues, is first and foremost focus on the serious threats. So the drug dealer on the corner is a threat, but he's not the same threat as the cyber exploitation. We need to put our focus on what are the serious threats.

We also need to know that secure communications are fundamental. They're fundamental for political discourse, they're fundamental for business discourse. And, as we know, they're

fundamental -- as we know on Valentines Day -- they're fundamental for private discourse.

The Preamble to the Constitution says that the U.S. Government should "secure blessings of freedom for posterity." When you build wiretapping capability into a switch, you're doing the exact opposite.

Communications surveillance should be designed with the idea of securing blessings of freedom for posterity in mind.

One of the things that happened under the last Administration is that a single person -- one single person sitting in the Department of Justice -- wrote a memo that said it's okay to wiretap warrantlessly -- for foreign intelligence surveillance. That got pushed up through the Attorney General, and for a period of five years, we had the warrantless wiretapping, with no public knowledge of it -- four years.

We should never have a system in place that one person can turn a switch and start wiretapping us. We need to have public vetting of security solutions, and we should also have a public agency supporting communications security.

The NSA is a very interesting creature. It's got communications intelligence, and communications security. And, in some

sense, they keep each other honest. But we don't have anything like that in the public sector, and it's something we need.

The FBI did a little bit of that, about educating businesses, but not enough. And, of course, it couldn't really, because it has a mixed mission.

We need to have that outside the Department of Homeland Security. And we need to have it, because it's important for both our freedom and our security.

So, with that, I look forward to Stu's response.

MR. BAKER: Let me try to respond to that quickly.

I think, you know, it was a very appealing suggestion that we had to -- we need to make technical changes to our architecture, or resist technical changes, depending on what you're proposing, because we all need security. And this is certainly the case. We do all need security online.

The difficulty I have is that it's an argument for building those -- that security in a fashion that it can't really be touched by even democratic governments, because it's built into the architecture of the technology we use. So that these changes are -- these policies are established, really, by the people who architect our technology. It's a kind

of geekocracy, in which the geeks determine whether we're going to have more security or more law enforcement.

And in some respects, that's what we've had for the last 20 years. I remember quite vividly the early days of the fight over crypto, in which these guys came in from the West Coast, couldn't believe we were going to get in their way at all. I mean, they wanted -- as they said, "We want crypto in your toaster, so that you can communicate with your toaster in case you need to adjust how brown it gets while you're driving home."

That idea, that we had to have the security, and that if we would just drop export controls on encryption, the geeks would deliver us security. And because we needed security, we should do what the geeks said -- was actually, in the end, after a long and bruising fight that left everybody a little chastened, it was the outcome that industry got.

And I'm sure you all realize how much more secure you are online than you were in 1995 -- right? The security that we were promised was never delivered.

However, Al Qaeda today has -- and many other terrorist groups -- have perfect communications security when they wish to communicate operationally. That capability has been widely spread. And it has been widely spread -- you know, we don't use crypto when we make

phone calls, because we don't really think anybody's listening. We may be wrong, but we don't expect people to be listening.

Terrorist groups do. So they have adopted this technology. We've gotten, in some sense, the worst of both worlds. We have widespread encryption available to everybody, but we don't use it because it's a hassle. And the terrorists do and, as a result, have perfect communications security.

This is not -- you know, this is not the world that was envisioned when we were being sold the idea that if we just got rid of export controls on encryption we would have a secure infrastructure. And that tells us that these solutions are often much more difficult, much more complex, than the people who are architecting them ever envision.

And I think, if I heard right what Susan was saying, she was saying -- "Lookit, we still need security. So, again, you should give me all of my policy choices, and then instantiate them in the technology so they can't be changed. We shouldn't have built-in wiretap capabilities because that reduces security. And we should instead take the anonymity technologies and the other security technologies that have been adopted by some portions of the U.S. government and push them out there as rapidly as possible so that we'll have security and all those people in Tahrir Square will have security. And isn't that a good thing? You want

them to have security, you want to have security, don't you?" And we all nod. And quite correctly. We do.

But the fact is that we will be providing security to the people who care most about it, who have the most to fear from authority around the world. And that often will turn out to be people who do not have the interests of anybody in this room at heart.

And if we make those decisions as a matter of architecture, we will regret -- as, indeed, I think we are regretting some of the architectural decisions that were made by privacy-loving, libertarian technologists in the '80s and the 1990s.

Let me talk briefly about attribution -- and I don't want to take too much time, so that we can begin the dialogue.

Susan, I think -- I give her credit for acknowledging that attribution really is important. Although, at the end, I thought she was saying, "Well, really, attribution isn't going to be the most important thing. What we need is security." And the implication was that somehow anonymity would give us security, or that we could get security by dropping CALEA as a mechanism for our protection.

And none of that, it seems to me, is correct.

Attribution, at the end of the day, is a critical mechanism for determining -- for establishing social order. And I think that's probably the most important part of our attribution, our approach to attribution.

If you look at how societies have dealt with the problem of maintaining social order, you can actually see this is remarkably built into our genome -- there are people who are so determined to enforce the norms of their society that they actually get pleasure -- get rewards in their reward centers for punishing people who have violated the rules that govern their society -- even if the people who are doing the punishment actually suffer as a result of that. It's a kind of altruistic punishment. And probably 60 percent of people do actually get pleasure from imposing pain on people that they believe have violated the standards of society. This is not news to anybody who drives in Washington.

But, what's significant about it, is that it tells us that punishment is at the heart of the way in which we have developed our society, and our social order. And we're not likely ever to be able to come up with a system in which we maintain social order without actually punishing people who violate the rules.

And it seems to me that when we look at the question of attribution, it's about punishing people who have violated the rules. It's about -- when you're looking at it at a nation-state level, attribution is

necessary in order to retaliate, sometimes massively, sometimes proportionately, to an attack that comes from a nation state. You have to know which nation state launched the attack.

This same thing is true with cyber espionage. If you want to punish countries that have engaged in cyber espionage, then you have to attribute the attack. You have to determine who is attacking you. If it's criminal hacking, you have to determine who has engaged in the criminal activity, and then subject them to prosecution -- arrest and prosecution.

All of those things depend on being able to attribute the attack and identify the attacker.

The kinds of attacks that you can stop just by building your defenses higher might consist of denial of service attacks. If I had to identify the kind of cyber attack I was least worried about, it would be denial of service. That is still largely solvable -- if you have big enough pipes or your ISP is sophisticated enough and you pay the ISP enough money. Whether that will always be true, hard to say. But today that is true. And so denial of service attacks are our least troublesome form of attack.

It's also the case -- as the guys in 4chan and Anonymous are going to discover -- it ain't a particularly anonymous way of attacking people, and there will be retribution. Those guys are going to get

arrested. And, indeed, they are getting arrested and prosecuted for launching the post-Wikipedia attacks.

So the question then becomes how do you get attribution in the current -- in our current system? And the answer is: not without making architectural changes.

And I certainly agree that there are multi-stage attacks, in which people move from one compromised machine to a second to a third to a fourth to a fifth -- all in different countries. But the answer, really, that Susan has offered to us is, well, you should follow legal process.

And I think it's fair to say that legal process as a mechanism for addressing that problem has completely failed. We have had, since the 1980s, an international policy of bringing people into a convention in which every country agrees that certain things are crimes, and they will quickly respond to requests for information as we try to track the attacker back from machine to machine, so that we can collect IP addresses.

I think it's fair to say that we are at roughly 15 percent of the world's nations have signed onto that. And the process still operates on a days or weeks basis, while the attackers are operating on microseconds.

And that's not likely to succeed if we continue to rely simply on solving the problem through our existing legal process. We're going to have to come up with mechanisms that allow attackers to be identified

across those multiple steps, rather than simply relying on old-fashioned legal systems that will never be able to catch up with the attackers.

Why don't I stop there, and I'll let Susan respond to that.

MS. LANDAU: Shall I --

MR. FRIEDMAN: We need a moment while someone comes and allows everyone to hear us.

MS. LANDAU: So, I don't know how you knew, Stewart, that I would want to respond.

So, I think it's a little bit disingenuous -- maybe I should let your expression be seen before I say it -- I think it's a little bit disingenuous for you to say that, "Gee, we haven't got any improved security over what we had in 1995," when the policies of 1975 to 2000 prevented the use of crypto in many things -- including, as I said, in cases of authentication and integrity.

MR. BAKER: The four people who were using the internet in 1975 might be aggrieved by that. But you properly set the bar at about 1992, 1994, when this became a debate -- and admitted that, by 1999, the policy had changed. It actually had changed for authentication before that.

But --

MS. LANDAU: But --

MR. BAKER: But we had 10 years in the promised land. Where the hell is our security?

MS. LANDAU: You know as well as I know how long it takes to get products out there. And we had -- and, in fact, even though it had changed for authentication and so on --

MR. BAKER: Have you looked at the apps market?

MS. LANDAU: But let me go on with some other points.

You said the terrorists have perfect communications security. Osama bin Laden does not use electronic communications, because we pick him up. Khaled Shaikh Mohammed got picked up through transactional information. That is how he was found in Pakistan.

There was a very interesting case in Switzerland, where the communication between two terrorists consisted of a phone call, the phone being picked up and then hung up. But they got arrested anyway. How come? Because these guys bought anonymous phone cards, and they bought them in a stack -- one, two, three, four, five, six, seven. And so law enforcement was tracking -- okay, card number one got used. Okay, card number two got used. And they tracked where the cards were being used.

It is not to say that the bad guys aren't using these forms of secure communication. If the only thing that wiretap did was kept the bad

guys off the networks, off the communications networks, that would be a wonderful usage. That's what happened with organized crime. Organized crime people did not use the telephones by the 1990s. You had to put bugs in their houses, because you couldn't tap them. I mean, you could tap them, but you didn't get anything.

That's a valid use. But it's not correct to say that the bad guys are all over their phone lines, because they're not.

MR. BAKER: They have perfect encryption.

I agree with you that the transactional information surrounding those communications is still a fatal flaw. That if you're a well-known terrorist, and you use modern communications, you're going to get a 500-pound bomb down your tunic.

MS. LANDAU: Right. Right. There was that interesting case in Yemen, where the NSA analyst recognized the voice on the call, and there was a drone that exploded the car very shortly thereafter.

MR. BAKER: Actually, I think it was on a seat. The guy was talking in the backseat, and there was somebody talking in the front seat, and he said, "I know who that is." Yes.

MR. FRIEDMAN: So, we're going to try, over the course of this discussion, to get out --

MR. BAKER: (Laughs)

MR. FRIEDMAN: No, no -- there are some times when the moderator knows just to get the hell out of the way.

But what I think it's important to do is get our terms straight.

So what we've done is we've said there's a difference between encryption and security. And we've learned that part of that is things like authentication, and part of that is things like auditing.

So we understand we have very good encryption right now, thanks in part to some of the work of you and your colleagues. And security is still a very big problem.

But to have a narrower view at the moment of the question of wiretapping -- what I'd love to do is get a vision of what you think -- roughly sketched out -- you'd like to see. What powers would you like to see? How far would you like to see CALEA extended?

And, alternatively, if we're not going to build backdoors into all these platforms, and bad people are using these platforms to communicate, how should we -- what should the law enforcement look like? What should the intelligence community have the power to do? And is it currently sufficient?

So -- want to start?

MR. BAKER: So I'll confess a moment of the ambiguity and ambivalence -- which I'm not known for.

MS. LANDAU: You're going to floor us all, Stu.

MR. BAKER: Sorry. Because, in fact, I think this is a hard one, and it may explain why the FBI, and maybe the Justice Department, can't get a bill out of the Administration.

It's very hard to see how you end up in a substantially better place, at a cost that you're prepared to pay, if you go down this regulatory road.

Yes, there are certain kinds of very mainstream telecommunications services that are not subject to CALEA. And it's very tempting to say we need to go after them. And maybe that makes sense.

The problem is, people who want to have telecommunications in the current system will be able to find ways to do that, using a variety of apps and software and the like, that will be almost impossible to control. Because they'll come from everywhere in the world, and you won't be able to stop them because they're simply selling -- or giving away -- software. And you can't prevent people from giving it away. You can't prevent people from installing it on their Android. And then they've got an open 3G network. They just use that for their telecommunications -- and you're screwed.

MR. FRIEDMAN: All right. And do you think there are directions that we should take?

MR. BAKER: I have a lot of sympathy for the view that when the FBI made the deal they made -- which is, “Okay. We’ll leave the internet alone -- that they made a choice that needs to be revisited. In fact, they have.

MR. FRIEDMAN: Yes, 2005.

MR. BAKER: They really have squeezed a lot out of CALEA that probably was not in CALEA.

And it might make sense to say, gee, why don’t we at least put what they already have in the law, and pick up some of the additional obvious, mainstream, telecommunications services that are being offered.

But I doubt that it’s really going to solve the FBI’s problem in a complete fashion.

MR. FRIEDMAN: All right.

Susan, do you have thoughts?

MS. LANDAU: Sure.

So part of the answer is, this has to do with money. But I want to start somewhere else -- which is that described a situation in which the NSA is living with the world as it is. And, obviously, they have ways of figuring out the communications they’re hearing -- or not hearing -- but figuring these things out.

The FBI and local law enforcement are case-based agencies. They get a case, they investigate it. They discover they can't wiretap, they're getting gobbledygook on the wiretap. They try to figure it out.

That's a very pressured situation. There may be lives on the line. It's a very frustrating situation. It's the wrong approach.

Back in 1996, the National Research Council produced a report, "Cryptography's Role on Securing the Information Society." Crisis Report. And they said then, the FBI needs a research arm to deal with advanced telecommunications. Instead of waiting until there's a case, the FBI guys should be doing what any researchers do. There should be an office within the FBI that goes to communications conferences, that goes to computer science conferences, that meets with the people doing startups, and figures out what the new, interesting communications technologies are, and develops tools for wiretapping them, so that the tool is available at the time the case comes up.

It's not going to be foolproof. Nothing is every going to be foolproof -- unless you make everybody use the old black telephone that I grew up with. And we're not in that world, and we're not going to be in that world anymore.

But that's the solution I would give.

Now, you're going to say, "That costs money. And we're in a time when we don't have money to spend." But any CALEA-type solution, any solution that builds wiretapping capabilities into switches -- whether digitally-switched telephone networks or the internet -- costs money. And it's a question of whether the consumers pay, whether it gets shifted onto the telcos and the service providers, or whether you say, "This is an important way for the FBI to maintain its capability -- without impinging on cybersecurity.

MR. BAKER: Well, I mean, I understand the appeal to geeks of having the FBI come out to them, on bended knee, or maybe holding cash, and saying, "Could you design your product so that it's more friendly to law enforcement?"

MS. LANDAU: I didn't say that, Stu.

MR. BAKER: But that's what you envision the FBI doing -- figuring out what's happening, and then hoping that if they go ask the geeks, that the geeks will respond.

But, you know, in my experience, about a quarter of Silicon Valley engineers would like nothing better than an opportunity to tell the FBI where to put it. And so the likelihood that they're going to respond -- especially if they can make a business case for security, which you always can -- strikes me as pretty modest. And the idea of having people kind of

build in, this way, that way, any which way, something they think will help the FBI strikes me as inconsistent with your concern that those sorts of solutions will reduce security.

MS. LANDAU: I'm talking about the FBI doing this in-house, in the same way that the NSA does it in-house. I'm not talking about the FBI bringing cash to companies. I'm talking about the FBI sniffing around and finding what new communications technologies are coming down the pike.

MR. BAKER: And spending whatever to takes to fix it.

MR. FRIEDMAN: And so we have set up, in the last five years, a number of institutions that span across governments, and that are supposed to bring in expertise from the NSA.

Do you think there is the possibility of cooperation on that level, to bring some of the technology from the intelligence side --

MR. BAKER: Yes, I actually --

MR. FRIEDMAN: -- down to the law enforcement side?

MR. BAKER: -- well, I do believe that law enforcement -- it's kind of embarrassing that law enforcement doesn't have the sort of centralized research capability and, you know, R&D approach that, say, DoD has. And I always thought that that would make a lot of sense, if not at the Justice Department, probably DHS should be doing that. They may

have more law enforcement people and more responsibility for local law enforcement than DoJ.

But it's almost impossible to persuade the people who run law enforcement agencies to invest in technology. As they see it, they're surrounded by opportunities to arrest bad guys. And if they've got enough money to hire four more guys, they could put more bad guys away.

And they are unable to resist that temptation, and disinclined to invest that money in something that will pay off -- if at all -- 10 years from now. And maybe, God forbid, for a rival agency.

MR. FRIEDMAN: Which, interestingly enough, this idea of how do you put the resources. You said it's always easy to make a business case for security.

I would argue, in the private sector, it's quite the opposite. If you can invest in information security against an unknown risk, you can also invest in new ways to improve your business processes.

MR. BAKER: Well, you're right. It is actually hard to sell security most of the time because it costs a lot.

My favorite story is the Air Force General who, when NSA went to him and said, "We've got this new crypto module and we want to install it in your planes," he said, "Well, I only want three things from your

crypto. It's got to be free, it's got to be invisible, and it's got to add a little lift to the plane."

That is the general security approach.

But certainly, the idea of building in a security hole -- a non-starter.

MR. FRIEDMAN: Well, and we've talked about building in a securities hole into switches.

MS. LANDAU: Right.

MR. FRIEDMAN: So now let's look forward to -- you know, we have someone basically saying, you know, people are using online games to communicate. People are using all sorts of things at the application layer. Which brings into play a couple of different questions.

One, information collection is often divided up into communications information, transactional information, and then data-at-rest.

Now, it seems to me, as we sort of mung all these into the application layer, it's much harder to disentangle them.

Can you give us any way of how we should think about them? Or should we get rid of those laws and bring in some new ways of thinking about how to gather information (inaudible).

MS. LANDAU: I don't think it's particularly hard when it's in the application layer to separate what the communication is, what the transactional information. So transactional information -- and I don't think we've properly defined it -- is the who, what, when of a communication. And it is often remarkably revelatory.

So I don't believe I said that -- a very interesting fact is that since the cell phone era, the U.S. Marshals Service now takes two days to capture a bad guy instead of 42, because all they have to do is see where his cell phone is at night, where his cell phone is in the morning, and look where family and friends are in that cell-phone sector, and then go to the apartment the second morning and they've got the guy, and they're on to the next case.

So transactional information picked up one of the London bombers of 7/21. Transactional information is really valuable.

But transactional information, content and stored data -- I think even at the application layer is not hard to keep separate. I'm not sure why you consider them "munged together." We'll have to talk off-line.

MR. FRIEDMAN: Okay. And just to push this a little further -

MS. LANDAU: Please.

MR. FRIEDMAN: -- from the case of industrial espionage -- if want to enable ready access to transactional data for law enforcement,

could this not also be useful for all of the malefactors we're talking about -- whether they're terrorists, or foreign military, or economic espionage?

MS. LANDAU: There is, as far as I can see, fairly ready access already to transactional information. Prospectively, it's a subpoena. Retrospectively, it's a National Security Letter. It's really readily -- and often the two are given at once. It's readily, readily available. I don't think that's a problem from law enforcement.

MR. FRIEDMAN: Okay.

MR. BAKER: As long as there's somebody you can safely serve the subpoena on, and they're not involved in the particular activity that you're worried about.

I agree. Right now, it's -- transactional data is saving law enforcement from a world in which it's harder to get content. But there's a vast amount of digital data about us suddenly available, with relative ease.

MR. FRIEDMAN: So, I want to move to some of the fun theoretical topics we talked about. Because whenever you have a discussion like this, you start talking about anonymity and attribution.

And, Stewart, your point about this idea of social regulation is near and dear to my heart. I love mathematical models of complex behavior.

But I wonder if you can sort of talk about how those can evolve, and how important we need -- what types of identity information? Can we have attribution at the IP level, as Susan mentioned? Do we need to have attribution going all the way up to the legal entity?

And how should we think about that in the face of threats like espionage and terrorism?

MR. BAKER: And I wish I had sufficient technical expertise to hold forth in detail on that.

It seems to me pretty clear that we're going -- one, obviously, you can't usually attribute beyond the machine. Although, increasingly, I think the machine will require that you identify yourself to the machine to use it, and you'll probably use your cell phone, and that will bring with it that sort of -- I always envision us as Pig Pen in the Charlie Brown cartoons. It's just this haze of data surrounding us, constantly sort of falling out and being generated.

And I think we'll start discovering that you could, in fact, identify the people behind the machine, getting access to some of that haze of data, some of which will be used to authenticate people to the machine itself.

But I fear, if you're going to have mechanisms to identify people through the multi-stage attacks, you've got to have a mechanism

that allows you to say either I can go right back to the ISP and get instant information about the hops that are occurring, or I need to start finding information added to the packets as the hops occur, that allows me to pursue that back to the original location.

This is a significant technical undertaking. And I don't know. I'm suspicious because 25 percent of Silicon Valley will tell me, "That's impossible," without having examined the technical possibilities. So I'm not sure whether it's technical -- something we can do technically.

But I don't see a solution beyond that.

If you cannot punish people who violate the norms online, sooner or later you will find that everybody has discovered there's a business model in violating those norms, and it will not be safe -- as increasingly it is not safe -- to do business online, to interact online. And as we put more and more of our lives online, more and more of our lives will be subject to more and more attacks.

Eventually we're going to say we can't live this way. And I think we should start designing a system that allows us to identify and punish wrongdoers. Because, as Susan says, it does take awhile to roll out.

I was struck by the fact that in 1996, I was told that U.S. encryption policy had failed because IPv6 had just been adopted, and it

was going to -- when it became universal, U.S. policy would be irrelevant. We are, of course, famously still waiting for IPV6 to be adopted.

MS. LANDAU: Well, IPV4 has run out of addresses. So it's now actually going to happen.

MR. FRIEDMAN: So -- Susan?

MS. LANDAU: So -- let me start with the attribution, because that's where we're having a conflict.

And I guess I'm one of the 25 -- I'm one of the 75 percent who's actually thought about the problem, rather than saying instantly "No." And the --

MR. BAKER: But you still came out in the same place.

MS. LANDAU: Yeah. Yeah, yeah, yeah. But I worked on it for awhile.

And the reason for the "no" is that as long as this is in a jurisdiction where you can continue to trust and examine -- you can look at the machine, you can look at the ISP, no problem. It's when it gets out of that jurisdiction, and you no longer -- you don't know what's happening there --

MR. BAKER: Right.

MS. LANDAU: -- and that's the problem.

MR. BAKER: So we do have a global internet. So we do have the problem -- right?

MS. LANDAU: We have the --

MR. BAKER: Are you arguing for a non-global internet?

MS. LANDAU: No, am not arguing for a non-global internet, Stewart.

MR. BAKER: I didn't think so.

MS. LANDAU: What I'm arguing is, that when the packets are traced to China, or to Russia, or to a bunch of other countries, at that point you lose the ability to trace them back further, because you can't get at the machine, and you can't at the ISP.

MR. BAKER: Right. Which is why you need architectural systems that actually do track it back, that they are not subject to political --

MS. LANDAU: So do you think your former agency would like the ability -- would like the entire network to be so transparent that any investigation they did could be traced back?

MR. BAKER: My former agency would hate that world. But at the end of the day, if I have to choose between security and the kind of espionage my former agency does, I think I have to choose security. We have seen --

MS. LANDAU: So we're flipping roles for a minute.

MR. BAKER:

MS. LANDAU: Let me push it a little bit further.

MR. BAKER: Quick -- get those wiretaps out of --

MS. LANDAU: Let me push it a little bit further and say that I don't think we could possibly see worldwide acceptance of such a protocol. I think technically it's very -- what you're describing is technically very hard, because the only way I could see to do it is to re -- I apologize for being technical -- to rehash and rehash and rehash. And you don't want to do that at the speed at which packets are going. So that's problem number one.

MR. BAKER: But computers are getting faster. Come on.

MS. LANDAU: Problem number one.

Problem number two is I don't see legal acceptance in large swaths of the world.

MR. BAKER: I disagree. I actually think most of the world is much less enamored of the lone libertarian standing up to government than we are, and quite happy to adopt --

MS. LANDAU: I wasn't thinking of the part of the world that cares about the lone libertarian. I was thinking of the part of the world that

cares not a whit about the lone libertarian, but doesn't want its activities chased.

MR. BAKER: Well, maybe they have to make the same choice that I just had to make.

MS. LANDAU: They control their pipes, and they're doing fine inside their countries.

MR. BAKER: And at some point you do say, "Fine, we ain't -- " --

MS. LANDAU: You want to stand up and support --

MR. BAKER: -- " -- we ain't taking your packets." Because I think that's what it comes to, at the end of the day.

MS. LANDAU: But we could do that now, and not have a problem.

MR. FRIEDMAN: So -- and I think the challenge for attribution is if we have this model where we can say, "Either you buy into this brand new, non-internet internet -- " -- I think it's often referred to as we'll have a green internet and a red internet. The red internet will be like what we have today, and the green one will somehow be magically secure.

So assume that we have one of those. Then if you don't buy into it, we can reduce the problem to a nation-state problem, and that's a

solid problem. And this is Richard Clark's approach to it, is saying let's just reduce it down to the boundary of the nation state, and then we can revert to the classic tools.

So, before we turn it over to the audience for some questions, I want to tie this in to whether or not we should care about whether other governments should care about the lone libertarian, or the lone freedom fighter, or the crowd of freedom fights. And get some sense from you on how important do you think it is to continue the U.S. efforts for internet freedom.

A report is going to be coming out this week to assess the Department of State's efforts, and try to suggest new directions. Is this something that we should really be pouring effort into? And, if so, does it send a mixed message when other parts of our government are focused on other aspects of the information infrastructure.

MR. BAKER: Well, I think the problem with the State Department's most extreme views is the sort of techno-libertarian psychological takeover that they've suffered.

So if you think -- if we just give these tools out, we'll free the world, you really are -- you know, you're channeling John Perry Barlow from 1995. You know, his day is over. And thank goodness.

But, the idea of letting tools loose that will allow people who are engaged in worthwhile activities to communicate securely is a good idea. But the idea that we should just say, “Oh, well, let’s find a security technology and release it,” let’s release the Tor, I think is probably the wrong solution.

And, indeed, a lot of the people who are trying to make sure information gets out securely have had to struggle with the question of, “How do I make sure this is not taken over by child pornographers?” And they have struggled with -- and in some cases, successfully struggled with that problem.

And I think that the State Department needs to look for mechanisms for dealing with this issue that are a little more nuanced than otherwise.

MR. FRIEDMAN: So, while I agree that we should look down on techno-determinists -- libertarian or not -- that, I think, is an orthogonal question.

I think that Tor -- the onion router that Susan talked about -- is actually one of the few examples where someone released a technology, a few people put it in people’s hands, and it took off like wildfire.

The challenge is, it doesn't scale to enable 3 billion people to have a global democratic dialogue. It's very good for small actors.

MS. LANDAU: Right. No, that one is an anonymizing tool about who's communicating with whom.

I was on a Federal advisory board a few years ago. And by statute, there's one member of the NSA on that board. He and I were the only holdouts of no cell phone and no E-Z Pass card because we didn't want to be tracked. But finally I had to break down because there are just no pay phones left anymore.

The FBI got scolded -- more than scolded, got a very negative report by the Inspector General, its Inspector General -- a few years ago for its use of Exigent Letters, which were an even weakened form of National Security Letters -- they were supposed to be followed up by National Security Letters -- to track people's transactional information.

And one of the striking examples to me at the time is that the FBI had reason to believe that a *Washington Post* reporter was speaking to terrorists, and so they wanted the reporter's list of communications -- not the contents, just who -- the numbers with whom the reporter was communicating.

But the order that got handed over to the communications -- that got handed over to the phone companies did not include dates on it. And so a much larger swath was given.

I can't think of anything more chilling to freedom of the press than that. And that's within the domestic United States.

So, we have moved from a world in which anonymous communication was very easy, because pay phones were on every corner, to the fact that even if you shut off your cell phone and use a pay phone -- if you can find one -- the French government actually tracks when cell phones get shut off and fake credit cards get used. So if a fake credit card is being used, they want to know all the cell phones in the area, and they look at which ones got shut off as it moved into the area, and they go after that person.

MR. FRIEDMAN: Digitally find the dog that didn't bark.

MS. LANDAU: That's right. Exactly.

So we have moved the whole world -- you know, in the same way that law enforcement finds itself going dark because of new communications technologies, privacy and anonymity has gone dark the other way.

And so I think the State Department -- to no surprise, I think the State Department responses are quite reasonable.

MR. FRIEDMAN: All right. I want to open it up to the audience for questions.

Just, if you could -- we have some mics coming around, and you can identify yourself and where you're from. And remember, of course, a question is short and ends in a question mark.

Ben.

MR. WITTES: Hi. Ben Wittes, from Brookings.

I'm fascinated by the idea of, you know, CALEA technologies as engineered security breaches. But it seems to me if you want to conclude that they have net security -- they cause net security loss rather than net security gain, you have to compare the aggregate loss to which they have contributed, and to which you can attribute to them, to the gains -- to security gains associated with the investigative products of lawful wiretaps.

And I'm wondering if you've looked into that at all? And how you -- I had the word "balance" in these contexts, but how you compare what the -- I mean, you were sort of dismissive about the idea that, you know, these are corner drug dealers that you catch this way. I suspect, you know, an FBI guy would say, "Well, wait a minute. We've done a lot with wiretaps."

I'm just interested how you compare the fruits of wiretaps under CALEA, with the engineered loss that you're describing.

MS. LANDAU: Right. So, very good question.

And part of the answer is I can't tell you which wiretaps occurred under CALEA and which ones not. I can't remember the number of Title III taps. I want to claim there are about 2,300, 2,400 a year -- under Title III, which are the criminal investigations.

I would like to say that 85 to 90 percent of them are organized crime. You do not see terrorism cases come up under the Title III taps. That doesn't mean a CALEA tap doesn't aid in a terrorism case, it just means that you don't get the data on it.

MR. BAKER: Well, but presumably, the same technology -- the CALEA-compliant technologies -- that's enabling the Title III tap is also enabling a FISA tap -- right?

MS. LANDAU: Correct. Correct. But we don't have any data on how many terrorism taps there were.

We also don't have any data on how important CALEA was to the actual tapping mechanism. That is, could the tap have gone through without CALEA? And there is no information on that, I'm sure.

MR. FRIEDMAN: And this is, I think, the key aspect -- maybe you can re-frame your question in terms of cost-effectiveness. Do you have thoughts on cost-effectiveness of different wiretapping regimes?

MR. BAKER: I think, at this point, it's hard to imagine that there are any wiretaps that are not enabled by CALEA. In metropolitan areas where wiretaps are most common, there's been a changeover in switches since 1994. And so all of them have been enabled by CALEA, and probably would be extraordinarily difficult, if not impossible, without CALEA. And so any wiretaps we do now are likely driven by CALEA.

Actually, what I think you would see at the local level is that a lot of state and local governments have been slowly priced out of the wiretap market. And --

MS. LANDAU: Not true, Stewart. The numbers --

MR. BAKER: Really?

MS. LANDAU: -- the numbers are actually higher for state and local.

MR. BAKER: They are higher, but I don't think they're as high as they were for state and locals back in the early '90s.

MS. LANDAU: They used to be close together. They're now higher.

MR. BAKER: Really? Okay. All right.

MS. LANDAU: Now, you may be right in the sense they might have gone much higher.

MR. BAKER: I'm certainly seeing governments basically get out of the business.

MS. LANDAU: But what -- I would disagree with you on CALEA-compliant, because the point is the switch is CALEA-compliant.

MR. BAKER: Right.

MS. LANDAU: But if the call didn't use any advanced network communication, then the wiretap would have gone through previously. And that's the part we don't know.

MR. BAKER: Oh, you mean if the -- okay. I'm not sure that's -- I even hear it correct, because the widespread use of mobile technology, which was basically un-wiretapable.

MR. FRIEDMAN: Nice thing about empirical questions is that they're answerable.

Jon, in the back?

MR. PEHA: Jon Peha.

I'm kind of curious about the characterization of onion routing, both as something we're afraid of that will be unleashed on the world -- I think was one comment -- or something that's caught on like wildfire, was another comment.

I actually don't think it's either. It's out there. It's in the world. And every day people do illegal things on the internet and don't use it -- for a variety of reasons.

MS. LANDAU: It's both.

MR. PEHA: But it is an early case of what we're talking about here.

I wonder if either of you would want to comment on what are the lessons, what are the costs and the benefits we've already experienced from onion routing as an example of this?

MS. LANDAU: So I think one of the very interesting benefits is that the entire code and the entire motivation and the ideas behind it are public. And there are attacks on onion routing. And then these guys go back and they work with the technology some more.

That's the way security technology ought to be. It should be public. It should be out there.

Let me give you an example of security technology that isn't.

The U.S. government is using Einstein 3 to protect the communications of Federal civilian agencies -- protect them against malware. And so it's an intrusion detection and an intrusion prevention system. And they use what are called "signatures," where they know what types of malware they can expect. There's lots of malware they can't

expect, they don't know about it yet, but they know some malware they can expect, and they just have to look at transactional information about the malware and then they say, "Nope. You can't come in."

Some of the signatures are classified. They come from the NSA. Reasonable that the signatures should be classified that a cryptographic key is not public information.

But the architecture of the system should be public -- should be open for public scrutiny in the same way that Tor is open for public scrutiny.

MR. BAKER: So, I was using Tor as an example of a technology which is pure capability, and has no ability to be shaped or restricted depending on the uses to which it is put.

And I think that's dangerous. And I think there's an infatuation with that in places like Silicon Valley and its exurbs that is not going to serve us well.

It is like crypto -- it's just enough of a pain so the only people who are likely to use it are people who really think they have to use it. Unfortunately, not all of those are, you know, budding human rights campaigners in Burma.

So that's my worry. I think we should be looking for, and the State Department should be looking for technologies that allow a little more social control than that.

I can't resist addressing Einstein 3. We've had 10 years and three Presidents tell us that Federal systems are under attack by sophisticated cyber espionage efforts and worse. And consistently, the response of the cyber libertarians is, "Oh, my goodness. That sounds like a bad thing. There must be something wrong with that. We think you should do something else." Something else. Whatever it is.

And, indeed -- not withstanding what Susan said -- the government, this Administration has, despite declaring a crisis, not implemented Einstein 3 because it is, in part, deterred by that strain of political and technological thought.

And the result of that is that we have massive attacks on our networks, in ways that basically allow attackers in all but a few agencies, to record officials' thoughts as they are typing them, to turn on their microphones, to turn on their cameras, and watch them in their offices.

Now, it happens that that's not the U.S. government that is doing that. But that is -- thanks, in part, to a cyber-libertarian campaign of making us afraid of 1984 -- that has delivered 1984 to practically every agency in the United States.

MS. LANDAU: So I need to answer that, Stu.

My understanding from talking to the folks at DHS is that the delay in deployment of Einstein 3 is they ran an Einstein 3 on a mid-level Federal agency and they ran into trouble. And so they couldn't scale. I don't think it was the techno-libertarians. I, by the way, am from Massachusetts rather than Silicon Valley, even though I used to work --

MR. BAKER: That would be the "exurbs."

MS. LANDAU: But it was technical problems in implementation.

MR. FRIEDMAN: It's also not clear to me that Einstein 3 intrusion detection-style systems would stop a ghost net-style slow --

MR. BAKER: Well, a lot of those ghost net attacks begin with malware. And you have to --

MR. FRIEDMAN: Sure.

MR. BAKER: -- identify the malware and repel it. And, indeed, Einstein 3 was held up for years over these libertarian privacy objections.

Of course there's always going to be a period in which you're struggling to make these things work. We're having that period now instead of three years ago, precisely because of the objections that cyber-libertarians raised.

MS. LANDAU: Not my experience.

MR. FRIEDMAN: Mike? Introduce yourself.

MR. NELSON: Mike Nelson, at Georgetown University and CSC Leading Edge Forum. I met both Susan and Stewart back in my days in the White House in the '90s, when we were trying to figure out Clipper Chip.

It was tough enough to deal with the domestic issues, but the international ones were far worse. And you've touched on those, but I'd like to go back to a couple of really important, hard problems.

Suppose we've figured out how to collect this data in the U.S.

MS. LANDAU: Which data?

MR. NELSON: Suppose we know how to track these people?

How do we share that? And with what governments do we share that data that we collect?

And then the other piece of this that I would like you to explore is: what kind of message are we sending to the rest of the world when we put forward these policies that say, you know, it's okay for us to close down WikiLeaks, or to cutoff companies that are hosting people who are doing things we don't like?

The case of WikiLeaks and Amazon is one, but DHS in the last couple of weeks have closed down dozens of companies because one part of the company was doing something that was deemed illegal.

So how do we get this balance right? How do we cooperate with those countries we should cooperate with? How do we move to some kind of global standard of taking action against illegal activities?

I mean, to put it bluntly, if the U.S. has the tools -- the U.S. government has the tools to listen in on somebody, do we share them with the Nigerian government? Or the Russian government?

MS. LANDAU: Well, you've managed me stump me, Mike. But let me try anyway.

So, there are many parts to your question. And I want to start with economic espionage.

So in the United States, economic espionage is a crime. Some of you probably know more about this than I, but it is certainly not a crime in more than three or four other countries in the world -- if it is a crime anywhere else in the world. I think the U.K. it may be a crime. But aside from that, it is not a crime elsewhere.

MR. BAKER: I don't think I'd try it in China.

MS. LANDAU: I don't think there are lots of things I would try in China.

But you can economically -- you can do economic espionage from China on other countries, and that's considered legal.

MR. BAKER: Yeah.

MR. NELSON: Well, but also --

MS. LANDAU: It's not legal for the U.S. to do.

MR. NELSON: Also, inside China it's --

MR. BAKER: It is -- that's an interesting question, whether it's legal for the U.S. government. They don't do it, but I'm not sure it's illegal.

MS. LANDAU: So I think -- so let me back up from a moment ago.

A few weeks ago Renault had a case in which three of its employees were alleged to have leaked information about their new electronic car, their new electronic engines, to China. And the French were very upset about it. It was very interesting to me, because the French have said quite explicitly that as far as the U.S. goes, in military and diplomatic affairs we're allies, but in economic affairs they consider us a competitor and an enemy, and economic espionage is quite legit.

I would really like to see a change in the world on that. That's a very grandiose idea. But perhaps with this quite shocking case to

the French -- because they really made a very big fuss about it -- we could begin to see a movement that way. So that's one answer, internationally.

On WikiLeaks, I read a wonderful paper by Yochai Benkler of Harvard Law, in which he discussed the sort of extra-legal efforts of the U.S. government. So, Senator Lieberman making comments about how Amazon and others should shut down WikiLeaks, and couldn't do it by the U.S. government but, by God, it happened. And what it looked like in the rest of the world. And it looked pretty bad. And the stuff was out there.

The other point that Benkler made is that the U.S. press appeared to exaggerate how many of the telegrams and so on were actually publicly available. He quoted press, and what they said, and what appeared to be the case.

The answer is it's very complicated, and I'm not going to give you very much of an answer. When I talk about attribution, when I give one of these technical talks and I do slides, I have a picture of China and I have a picture of France. Or have a picture of China and I have a picture of the U.S. And in one country free speech is legal, and economic espionage is a crime. And in the other country, free speech is not legal, and economic espionage is allowed.

The internet has made international communication easy, but not in the way that we expected 15 years ago. You can't stuff into

Burma, and the stuff in Singapore is tightly control. And add China -- well, some stuff goes out, but not exactly what you expect, and so on.

And so I don't think there is a five-minute or even 50-minute answer to your question, so I'll stop here.

MR. FRIEDMAN: We're working on it. So -- sharing information and technology.

MR. BAKER: So -- yes, in my experience -- especially in law enforcement, but also in intelligence -- there are really no more brutally reciprocal relationships in the world. We should share with the people who share with us. And we should do unto others what they do unto us.

I have to say I think that's our only hope. And I don't think we have a lot of hope. Certainly, hoping that economic espionage will become less frequent because the French have discovered they're on the receiving end of it is, I think, an illusion.

In fact, you get economic espionage by sophisticated governments whenever you have mercantilist states with heavy interconnections between the government and industry. And we've seen the rise of China with just such a system in the last 10 years. And that makes the likelihood of economic espionage far more serious.

I, you know, bid for some area of agreement. I'm going to ask Susan when I finish this if she agrees with me that maybe we should not be buying telecommunications equipment from that country.

MS. LANDAU: No "maybe" about it.

MR. BAKER: Yeah. Okay. Good. Then we agree on something.

MR. FRIEDMAN: Fine. Where are you going to buy them from.

MR. BAKER: Well, from the Finns, probably. Or the Swedes -- which is, you know, on the whole, better than the alternative. The French are still in there, though.

The other question -- well, what should we be doing? And how do we look to the rest of the world?

I'll seize this opportunity to says that DHS has to have something better to do than seizing web sites devoted to, you know, offering people who want to buy fake trademarked goods, fake trademarked goods. That's just bizarre. And their effort to do that is, you know, a sign of how our intellectual property rules have sort of gone off the rails.

I do think it's a little odd that if the WikiLeaks had been posting Rihanna albums they would have been shut down by every one --

you know, Amazon.com could not have kicked their butt off of their system fast enough. And the idea that Rihanna gets more protection that Hillary Clinton is, I think, a little bizarre.

So my modest proposal in this -- and maybe we can agree on this -- is that surely when Julian Assange writes his book, we should not allow take-down orders to be sent to the web sites that make it available for free to the rest of us.

MR. FRIEDMAN: We'll just have to put a quick note just to show that Stewart has many interesting positions. He's the only person I know who has written a book which is not terribly kind to the Electronic Frontier Foundation, but is published under the Creative Commons License, and is thus available for free download on the internet. So he does --

MR. BAKER: You can pay for it, too, by the by.

MR. BAKER: -- he does put his money where his mouth is.

I think we have time for one last question from the audience. In the back. Sorry -- the gentleman with the mustache.

MR. WILLIS: Yes -- John Willis, independent privacy and security consultant.

Do you see any -- or what value do you see in promoting the use of trusted computing environments for consumer PCS, especially when they're entering regulated environments?

I think, briefly, of a scenario where you consider them like a person driving a car, needing a driver's license, you know, registering their vehicle -- that sort of thing. You know, for example, would requiring registering your PC key with an ISP be an interesting avenue to go?

And just forward thinking, do you see any of those technologies being of interest?

MS. LANDAU: So --

MR. FRIEDMAN: You have two minutes each on trusted computing.

MS. LANDAU: So, coming clean, while I was at Sun I did some work for Trusted Computing Group and, in particular, I was responsible for the best practices. Now, how they're being implemented is different from writing the best practices, but it took enough time to get them through that, at least at the time we did, it was understood that they had real teeth in them.

And they talked about usability. They talked about data portability. They talked about privacy. And I would urge you to go to the

TCG -- the Trusted Computing Group web site -- and find those best practices, 1.1, or 1.2, whatever version it was.

That said, one never knows how the implementations happen. And, in particular, TCG never set up a process by which the standards had to go through a measurement against the best practices. So the best practices were official, and officially part of the standards -- and they were privacy protective, and protective of users' rights. So, in particular, it said the TPM and the TCG technologies should not change the ownership model of data. And usability was in there because, of course, if you make it sufficiently difficult to sue it, then things get changed on ownership without the user intending.

So -- strong set of best practices. But whether they were actually -- whether they are actually being implemented in the standards being promulgated by the group is not clear.

MR. BAKER: So, very quickly -- I think, in the end, if you want to hook up to a network, you're going to have to live by the network's rules. And that means surrendering a lot of autonomy over your machine.

The good news is that CPUs are cheap. I think I brought two with me, and I didn't bring a laptop. You know, you just carry them around everywhere. There's no reason why you can't have one CPU that you use

to traverse Tor, and another that you use to, you know, hook up to the network that is trusted and abide by its rules.

And that's perfectly legitimate. And, of course, they should require you to turn on your TPM, and they basically can tell you what you can and cannot install on your machine -- as they should if they want to be able to control and secure their network.

That's how we're going to end up building whatever islands of security we find ourselves living on. Because gradually we'll build networks -- we'll tell people, "If you want to be part of this secure network, you have to give up a whole bunch of anonymity and autonomy over your machine." But the good news is, you won't be ripped off every 20 minutes.

And I think most of us will take that solution, most of the time.

MR. FRIEDMAN: And, in fact, the evolution of security in a complex environment is one of the main focuses of the Center for Technology Innovation here at Brookings.

And I would like to thank you for all joining me this afternoon, and ask you to join me in thanking Susan and Stewart for their discussion.

Thank you.

(Applause)

* * * * *

CERTIFICATE OF NOTARY PUBLIC

I, Carleton J. Anderson, III do hereby certify that the forgoing electronic file when originally transmitted was reduced to text at my direction; that said transcript is a true record of the proceedings therein referenced; that I am neither counsel for, related to, nor employed by any of the parties to the action in which these proceedings were taken; and, furthermore, that I am neither a relative or employee of any attorney or counsel employed by the parties hereto, nor financially or otherwise interested in the outcome of this action.

/s/Carleton J. Anderson, IIi

Notary Public in and for the Commonwealth of Virginia

Commission No. 351998

Expires: November 30, 2012