THE ASPEN INSTITUTE

ASPEN SECURITY FORUM: GLOBAL

CYBERSECURITY: THE NEW FRONTIER

Lancaster House
Stable Yard, St. James's
London, United Kingdom

Friday, April 22, 2016

LIST OF PARTICIPANTS

CLARK ERVIN
Director, Homeland Security Program,
The Aspen Institute
Partner, Squire Patton Boggs

STEWART BAKER
Partner, Steptoe & Johnson, LLP
Former Assistant Secretary for Policy
Department of Homeland Security, United States

SHAMI CHAKRABARTI
National Council for Civil Liberties

DAVID SANGER
Moderator, Chief Washington Correspondent
The New York Times

* * * * *

CYBERSECURITY: THE NEW FRONTIER

(4:45 p.m.)

MR. ERVIN: So this session is titled *Cybersecurity: The New Frontier*. I guess it should be called the New Old Frontier. Frank Gardner was quite right in saying that you can't talk about terrorism and counterterrorism without talking about cybersecurity. But cybersecurity is not just a matter of terrorism and counterterrorism, there's also, of course, cyberespionage, cybercrime, and perhaps someday, God forbid, cyberwarfare.

To moderate this afternoon's session we're very pleased to have an old friend of The Aspen Institute with us, National Security correspondent for *The New York Times*, and one of the paper's senior writers, David Sanger. David is the author of two bestsellers on foreign policy and national security, the 2009 book, *The Inheritance: The World Obama Confronts and the Challenges to American Power*, and the 2012 book, *Confront and Conceal: Obama's Secret Wars and Surprising Use of Power*. And finally, he has twice been part of *New York Times'* teams that have won the Pulitzer Prize. Please join me in welcoming David Sanger, who will moderate this discussion.

(Applause)

MR. SANGER: Well, thank you very much. It's great to be back here. It's great to be back at an Aspen Security Conference event. The last one of these that I moderated, I think the risk of this today is fairly small, we all came in and we sat up nicely on the stage after a nice coffee break, and then somebody discovered that a bear was walking out on the patio where we had all just been to clean up our leftovers from the coffee break. I'm told that this does not happen within the confines of St. James Palace very often.

(Laughter)

MR. SANGER: We have other risks.

MR. ERVIN: The automatic weapons (inaudible).

(Laughter)

MR. SANGER: So it's great to be here, with an old friend, Stewart Baker. I was a partner in Steptoe & Johnson, was the Assistant Secretary of Policy for Department of Homeland Security. And with Shami Chakrabarti, who was, until recently, I guess, Director of the National Council for Civil Liberties, here in London. And so we sort of envision a two-part conversation before we open this all up to you. We want to pick up a little bit with where you left off last night with Director Comey, and sort of use the Apple case as a jumping off point to talk about where some of these issues are going from here, both in the United States and in Britain, and more broadly.

And then we're gonna pivot a little bit to, as Clark suggested, to questions of state conflict involving cyber. You know, cyber's really got these two major elements to it. There's the security versus privacy issue, and then there's the security versus security issue as both the US and Britain, though they don't like to talk about it very much, turn to cyber weaponry, and begin to make use of them as they have begun to make use of them, say, against ISIS, but not exclusively there.

So Stewart, let me start with you. You were here for Director Comey. I unfortunately was still stuck in an airplane, but I've caught up on the news where he described how much money they spent breaking into an iPhone that appears to have given them absolutely no information at all. But separate and apart from that, tell us what you thought you heard different, if anything, from Director Comey from what we've all been hearing as this drama over the iPhone and the effort to force Apple to try to open it up has played out in the United States.

MR. BAKER: I don't think there was much that was different apart from the seven times his salary remark about the cost of this. He is a --

MR. SANGER: Thus revealing how we underpay public servants in the United States.

MR. BAKER: Exactly.

(Laughter)

MR. BAKER: He's a very gracious and effective spokesman for his point of view, and his basic point was we've always relied on law and judges to protect our privacy and to decide when the criminal authorities ought to be able to invade that privacy in pursuit of evidence. And we now face a world where technology can say to the law and to the judges it doesn't matter what you think, this data is outside of the capability of law enforcement to obtain. He's been making that point for a year now, and that was roughly his point again.

MR. SANGER: So Stewart, that has been his point for a year, but it strikes me that the US Government has never effectively addressed Tim Cook's best argument out here, which is let's say we do this for you. Let's imagine a world in which we create some way which Director Comey does not want call a back door, but whatever kind of -- we come up with a way that the company can get you in. He says you're going to get in when the judges ask you to, and you're going to look over shoulder, and the Chinese are going to be right behind you. And you're going to look over the shoulder, and the Russians are going to be right behind you. And then the Iranians are going to come in. And there's no way to design this, much as you may want to wish it away, so that you're not allowing an opening that somebody else is going to get into. And it strikes me that that argument has been bolstered by the fact that for $1.3 million, plus, they actually found a way already.

MR. BAKER: Right. So I actually think there are two arguments that have been going on. His original fear was that companies would release encryption that they couldn't break themselves, that if you set it up, you would be the only person that could get in it, and the company would be unable to assist law enforcement when they came to them. And there's a very robust and appropriate debate over whether it's proper to ask companies to build in some capability to get access. It's a tribute to Apple's marketing prowess that they've kind

of hijacked that argument, because they can get into this phone. They know how to do it. They could design a mechanism that would allow the law enforcement to get in and make it available on a retroactive basis. And they just choose not to. And their decision that that they don't want to do this is being treated, is being, I think, mixed with the question of what if they had built something that they really couldn't get into. And the problem in all of these arguments is Apple can get into this phone. And if that's the case then the Chinese can line up behind them no matter what the FBI does, and tell them, "You can get in. Do it or you lose your most lucrative market." And they have made many compromises with the Chinese authorities, and will make more. They've just been given a taste of what they could lose in the Chinese market. And so their argument that --

MR. SANGER: For the audience, the Chinese for the first time have banned what, iTunes --

MR. BAKER: iTunes and their books, if I remember right.

MR. SANGER: Yeah.

MR. BAKER: Their bookstore. Right.

MR. SANGER: And until now China's allowed just about everything that Apple wanted to put on in the way of --

MR. BAKER: Yes. Although, they have occasionally -- they had a big campaign against Apple's iPhone for about three months, and then Apple arrived at some kind of unspecified compromise with them over how it was going to be handled, and all of those objections went away. So we don't fully know what compromises have been made, but it's likely that there have been substantial ones, and that they will continue into the future.

MR. SANGER: Okay. So Shami, you've been watching this Apple debate play out in the United States. From our earlier discussion, it sounds like with some mix of fascination and horror. So let's imagine a world in

which this had broken out not in San Bernardino, and all that, but in London, over a terrorism case similar to what you had in the tube a number of years ago, or any other kind of terror case you could imagine. How would it have been different?

MS. CHAKRABARTI: Well, thank you. First of all, welcome to my city.

MR. SANGER: We're glad to be here. You all live like this every day, don't you?

MS. CHAKRABARTI: Absolutely.

MR. SANGER: Yeah.

MS. CHAKRABARTI: Absolutely. Welcome to my living room. No.

MR. SANGER: Yeah.

MS. CHAKRABARTI: And secondly, apologies to the Americans in the room for the ill-judged remarks of our mayor today in relation to your president. This is a great international city, and it's a city and a country that greatly values the special relationship. And we're not all xenophobes or racists.

Secondly, in relation to the whole Apple thing, I think it's been a really important case that's triggered a really important and refocused debate, because it's been so easy for so long to pit national security, as we call it here, or homeland security, as you call it there, against civil liberties or privacy. So what we see through the lens of the Apple-FBI debate is an increasing realization that national security, or homeland security, is in no small part the personal cybersecurity of millions and millions of people all over the world.

And if I were, you know, a hostile power, state or non-state isn't even the principal issue any more, if I were a hostile terrorist organization or a hostile foreign power I would be interested in undermining the cybersecurity not just of state institutions, but of

individuals in causing the kind of crisis of trust in the banking system, in the tax system, causing panic, because that's a really good way to terrorize people.

And so, you know, I appreciate using some -- you've been talking about bears. Let me talk about hawks. In certain hawkish circles it must seem like Apple is just being completely petulant and ridiculous, but they must be concerned about the potential crisis in trust and calm in their products and in their systems if they let on to millions of Apple customers, like me, that their systems are not secure, or could be so readily compromised, or would be so readily compromised by the company in which you place your trust.

Now governments, I heard Charles Farr earlier say, "Well, actually, the public's very happy to trade privacy for security. The polls all say that, but the corporates don't believe it." Well, you know, the corporates have rather a lot at stake. And governments seek reelection every so many years, you know, four or five years. But the corporates could potentially lose trust, lose consumer trust, and lose millions, and millions, and millions of consumers and pounds or dollars in a lot shorter period. And so they are having to have -- yes, they have to have concern for supporting the authorities, but they have to have a principal concern for retaining trust, and the security, and the good will in the personal cybersecurity of all of those customers.

I don't think it's so easy and Apple's necessarily so petulant. Here, if this case had emerged in London instead of San Bernardino, which was the hypothetical that you picked --

MR. SANGER: Uh-huh.

MS. CHAKRABARTI: -- it would be really interesting, and the timing would be important. But as I suspected if it happened now, before the Investigatory Powers Bill had passed, there would be a good old fight in the courts as we've seen (inaudible).

MR. SANGER: I was about to ask you about the

Investigatory Powers Act. So you'll remember that a year ago Prime Minister Cameron came out and basically said we're not going to allow products that we can't get into. Then he had to back off from that a little bit.

MS. CHAKRABARTI: Indeed.

MR. SANGER: And then the Investigatory Power Bill came together.

MS. CHAKRABARTI: Which includes --

MR. SANGER: Just tell us what that would do to change --

MS. CHAKRABARTI: Well, there's so much in that bill that we don't have time. I find it a breathtaking piece of job legislation. Whatever you think of Mr. Snowden, right -- some people think he's a public interest hero and whistleblower. Some people call him a traitor. Whatever side of the argument you're on, I've got to say this for his revelations. That until he made those revelations the practice -- maybe the practices were perfectly justified and proportionate, but they were not conducted with public knowledge, or debate, or consent, or parliamentary, or political knowledge or consent, let alone with the rule of law. So what he revealed, in my view, certainly to those of us in the legal and civil liberties community in the UK, is a breach, not just of the rule of law, but parliamentary democracy itself. So now we have this bill, which, in part, is designed to legitimize what was happening. Instead of saying, "Sorry, hands up," it's, "Well, now we're going to write the check for the money we've already taken."

MR. SANGER: But Shami, would it require Apple to have a --

MS. CHAKRABARTI: There are powers in that bill. There are lots of breathtaking powers in that bill, but in particular there are powers in that bill which would allow the government to order Apple to build in backdoors into their products and their systems, as is one of the many very controversial and I would say concerning aspects of

that bill.

MR. BAKER: If I could –

MR. SANGER: Sure.

MR. BAKER: What's interesting about Snowden and the Snowden effect on Silicon Valley is that the principal victims of the Snowden effect have been the law enforcement authorities of countries like the UK. Because the first thing that people did was say we have to make sure that TLS encryption between the user and the server that they're going to is unbreakable, even by the companies.

MR. SANGER: Do you want to describe TLS encryption?

MR. BAKER: Basically it creates an encrypted pipe between you and the Gmail server that you're getting your mail off of, or *The Washington Post*, if you're reading the *Post*. That encrypted pipe is unbreakable, and it didn't exist with enthusiasm, wasn't adopted with enthusiasm until the Snowden revelations. The United States, because much of this material is still in the United States, the United States can still serve court orders and read the mail of suspects on the server, but if you are the British authorities, even if this is mail between two British terror suspects, you can't get into that. You used to be able to wiretap that line. Now you can't. You cannot read that unless you can get the cooperation of Microsoft or Google.

MR. SANGER: This is data in transit.

MR. BAKER: Exactly. And so the British authorities really felt the lash of mandatory encryption, and that has led them to think about can we break the encryption, can we force people to give us keys, or can we exercise extraterritorial authority over Hotmail and Gmail, and force them to give us this information from their servers.

MR. SANGER: Well, that raises an interesting question. So Shami, supposing I've got my mail on a Gmail server sitting in the United States, and the British authorities, for some unknown reason, want all the photographs of bears of Aspen out of my iPhone.

(Laughter)

MR. SANGER: Can they go through the courts in Britain under the new law, and pull something from a server that's not in Britain?

MS. CHAKRABARTI: Again, one of the more controversial aspects of the bill, it's not yet law, but when it was first published one of the more controversial aspects, including the one mentioned, is the extraterritorial aspect.

MR. SANGER: And it would essentially allow the British authorities --

MS. CHAKRABARTI: Yes.

MR. SANGER: -- do what the US Justice Department has been asserting it can do --

MS. CHAKRABARTI: Yes.

MR. SANGER: -- with respect to Microsoft when Microsoft stores the e-mails in --

MS. CHAKRABARTI: (Inaudible). It's a shrinking interconnected planet in so many ways, and this is never truer than in the virtual world. As you say, the US authorities have asserted, you know, the (inaudible) and now, you know, the UK Government is seeking to (inaudible)

MR. SANGER: Well, let's pull on this string for a moment. So you've got a wall coming together in Britain that will be passed, it looks like, by the end of this year, that would allow Britain to go into a server that's not on British territory. In the United States, as

Stewart suggested, there's a case under way called the Microsoft Ireland case, where Microsoft has got store's e-mails for European customers in a server that's sitting in Ireland. They got a subpoena in what we believe was just a pretty routine drug case. They said, "Very good. Take the subpoena and give it to the Irish courts," and the FBI and the Justice Department said, "No. No. No. You're Microsoft. You're an American company. You have to give us the data no matter where you store it in the world."

MR. BAKER: Right.

MR. SANGER: And that is now in the Second Circuit, as I recall.

MR. BAKER: Yes.

MR. SANGER: And we're sort of awaiting it. It's been argued. We're awaiting a decision. So let's assume for a minute that the government continues to win its case as it did in the lower court. And let's assume for a minute that the bill goes through as it currently has. So then you have a precedent in Britain and the United States for extraterritoriality. So Stewart's Gmail next is stored in a Chinese-owned server sitting in a cornfield in Iowa. And those highly independent Chinese courts decide they're really interested in Steptoe's business, and the go through the Chinese courts to pull the data out of the United States. Can you imagine that happening in the future?

MR. BAKER: I could imagine that happening. You know, for a long time we had this very fragile consensus that where the servers were, where the data was stored would establish the law that governed the data. And that is breaking down in every way possible. And the new principle that probably takes its place is if the company that stores the data is subject to the jurisdiction of Zimbabwe, then Zimbabwe gets to tell that company to cough up the data.

MR. SANGER: Which is fine if we're all living in a world in which we have trust in the court systems, as Britain has in the United States courts, and the US has in the British courts. It falls down when you're dealing with authoritarian regimes, whose influence over their courts are pretty high.

MS. CHAKRABARTI: If ever there were a need for, yeah, a new truly international settlement around issues of this kind I think it has to be in relation to internet communication.

MR. BAKER: But that would require the governments to agree, and they would also agree that they'd have to get access.

MS. CHAKRABARTI: Yes

MR. SANGER: That's right. OK. In the few minutes we have before we go out to questions from the audience, and I'm sure based on what we've just described we'll have more than a few, let's turn for a moment to how governments are using cyber as a weapon of influence, conflict, and so forth. Stewart, as you and I have talked about before in your podcast series, which if all of you don't listen to, Stewart does a great -- weekly?

MR. BAKER: Weekly.

MR. SANGER: Weekly podcast on cyber issues that you can listen to while you're on the exercise bike, or wherever.

MR. BAKER: And knowing this audience, at least half of you would have your heart rate increase just by listening to it.

MR. SANGER: That's right.

(Laughter)

MR. BAKER: In fact, you can get off the bike and not do any exercise at all.

MR. SANGER: Exactly.

(Laughter)

MR. SANGER: It would certainly be my preferred way. So we've had the government in the United States and a government in Britain, that both have built up considerable offensive cyber capabilities. In the US we have the United States Cyber Command, which is the sort of military sidekick to the NSA. They're putting together what they call national mission teams. These are essentially the special forces of cyber. And while they've never discussed their missions before, in the past two or three weeks we've suddenly had President Obama, Ash Carter, the Secretary of Defense, other officials say, "Hey, we're using this against ISIS." This is a bit of a change, isn't it?

MR. BAKER: Yes.

MR. SANGER: Because until now there has been something of a debate about whether we even want to use cyber as a routine element of your military forces.

MR. BAKER: Yes. I think that's exactly right, but what is striking about the cyber weapon is what I think Stanley Baldwin, and the last time an English-speaking politician actually told the truth to his populous, said, "In the next war the bomber will always get through. Our wives and our children are going to be killed in their homes in the next war, and the only way we'll win it is if we kill their women and children faster than they kill ours." It is an inherently offensive weapon right now. Our defenses are just miserable. And so there has been both an enthusiasm for using it because of its enormous power, and a fear that if we started using it routinely we would end up unable to defend against it. And so I think what this is an effort to do is to demonstrate that actually we do have a very strong

offensive capability in the hopes of deterring not ISIS, but countries with more capability, North Korea, Iran, to make them think twice before they use their weapons.

MR. SANGER: Don't the Iranians get this already? I mean they were the subject of a significant cyberattack engineered by the United States and by Israel, so it's not a surprise to them, or to the Chinese, or to the Russians that we've got all kinds of cyber weapons.

MR. BAKER: Right. And I think the Iranians have been going through an exercise of how about this, is this bad enough, or is it okay. So they have been doing denial of service attacks on our financial system. They have been breaking into dams, and tweaking the controls, just to see if we would take that badly enough to actually attack them. And thus far we have exercised a lot of restraint.

MR. SANGER: So Chami, what strikes me is I watched the discussion about using cyber weapons in the United States, and Britain, and Israel, and elsewhere, the other countries that are capable of it, is that in the US we're beginning to have a debate. The government hasn't participated in it much, but we're beginning to have a debate. How about here, where the capability lies largely in GCHQ, where the official Secrets Act means that they know how to deal with people like me.

(Laughter)

MR. SANGER: So what's going on in the debate here?

MS. CHAKRABARTI: I don't think we have the equivalent mature debate, if I'm honest. We have a greater culture of secrecy and tradition of sort of reverence, and respect, and trust, which I think is changing, but not quickly enough. And I think that technology moves a pace, and the political, ethical, legal debate doesn't catch up.

MR. SANGER: What's fascinating to me about that is that so many of the Snowden papers that got released were, in fact, GCHQ documents --

MS. CHAKRABARTI: Yeah.

MR. SANGER: -- that laid out what GCHQ's capability was here.

MS. CHAKRABARTI: See, I think some people would almost treat it, some people in Britain would almost treat it as no debate when, when we're talking about, you know, theoretical cyberattacks on hostile powers, or even on, you know, Islamic States. Interesting, isn't it? Because we don't want to legitimize that movement as a state, but at the same time we want to treat it as a state for the purposes of -- there's a whole tricky philosophical area there.

MR. SANGER: Stewart, this raises a really interesting question Chami has brought up here, because when I ask people in the US Government, "So how come you guys are suddenly talking about this?" I've gone through seven years with trying to make people talk about this, and I get doors slammed in my face. Okay? So now it's happening. And the answer I get back is, "It's a very different thing to talk about attacking a terror group where we recognize no sovereignty, than talking about doing an attack on a nation state, where we are getting it."

MS. CHAKRABARTI: This is exceptionalism, isn't it? This is post-9/11 exceptionalism, because tradition -- I'm not a pacifist, and, you know, people who believe in the post-World War II human rights settlements are not necessarily or predominantly pacifists. But even in war we believe in rules. There are rules even in war. Question number one: Are there going to be rules in this kind of war? And question number two: What are we going to do to ensure that this kind of war doesn't creep into a normalcy that isn't just about war situations against hostile states, where we've been honest about the fight

that we are at war, but creeps into a compromise to corporate security, personal cybersecurity on a more routine basis?

MR. SANGER: So Stewart, do you believe that by talking about this in relation to ISIS the government is doing just what Chami suggests, and beginning to get Americans accustomed to a normalcy in which you use drones, you use conventional bombs, you use cruise missiles, and you use cyber, and you just put them all together?

MR. BAKER: So I think most people would say if you can use cyber weapons and kill fewer people, target them better, inconvenience terrorists, that's great. Better that --

MS. CHAKRABARTI: Sure.

MR. BAKER: -- killing people. So I'm not sure as a --

MS. CHAKRABARTI: You still need rules, don't you?

MR. BAKER: Well, you know --

MS. CHAKRABARTI: Because what if you're the person that is the terrorist or the suspected terrorist? You would want there to be --

MR. BAKER: Well, yeah.

MS. CHAKRABARTI: You would want there to be some rules.

MR. BAKER: I suppose. I would want to be aggrieved by the fact that my computer has been bricked, and so I can't send Tweets encouraging people to join ISIS. You know, on the whole, I don't think they recognize our --

MR. SANGER: But Stewart, that assumes a computer on computer attack, and ask the Ukrainians, who woke up on, you know, Christmas week and discovered that some computer hack had taken out their electric power.

MR. BAKER: That's right. So there are certainly bad things that could happen, and we could take out power, I suspect, in Raqqa. But, you know, we've done more than -0

MR. SANGER: If it would ever go on we could take it out.

MR. BAKER: Right. We've done more than that already in response to cyberattacks by ISIS. ISIS hacked a list of US military forces' personal data, released it on Twitter. Al-Brittani released it on Twitter and said, "Hey, you got your list, now we've got ours." And he was killed in a drone attack two weeks later. And two months later the guy who did the hack was arrested. So we have already started to bring pain outside of the cyber area to ISIS relating to their cyber-attacks.

MS. CHAKRABARTI: But my point is simply that post-World War II we believe in domestic and international rules of law, and even when one is fighting an enemy there are certain rules about proportionality, and about what the processes are for determining who is and is not a legitimate target. Now you're quite right that on the proportionality point I would rather be hacked than killed. Rightly or wrongly mistakenly or correctly, I would rather be hacked than killed, but I'd rather not be hacked if I wasn't actually, in truth, and on the evidence, a legitimate target.

MR. BAKER: If anything, to my mind, the US military has been tied up unduly by a desire to make more rules in this area, an area where we really don't even known what works and what doesn't work, and so the question of the efficacy of particular attacks can't be answered until we have a good deal more experience. Yes, of course, you know, turning off the power for two months

to a major city is going to cause massive harm to the population --

MR. SANGER: And death.

MR. BAKER: -- millions, total breakdown in civil order. And you would only want to do that in a context where it was enormously important from a military point of view. So there are some basic rules that everybody could agree upon, but the idea of bringing the full panoply of the laws of war, or international laws of sovereignty and jurisdiction to bear on such an infant military weapon I think means that we simply will be not allowed by the lawyers to use it in context where it makes sense.

MR. SANGER: Very good. So we've got about 10 or 15 minutes left to take your questions out here. So why don't we start right down here. There's a microphone coming to you. Tell us who you are, and --

MR. GIVELLI: My name is Mark Givelli (phonetic), and I'm a student at Oxford University. You mentioned the logic of deterrence, and sort of how the development of these cyber weapons is playing out. I'm curious, where does that logic begin to break down in terms of properly IDing or properly sending the messages out of how you can retaliate, and the nature of the weapons. And also, is it necessarily the best way to conceptualize it in a model of deterrence or potentially in more of a global commons, where you start to push the boundaries of sort of civilized safe spaces, and to have countries sort of patrolling the oceans, the global seas, if you will, on the internet?

MR. SANGER: If I understand, the first question is basically an attribution question. Is that right? How is this a deterrent if you can't truly attribute where an attack comes from?

MR. BAKER: Yeah. So attribution has traditionally been the problem. You can't get deterrence

if you can't identify and punish the right person. I am trying to popularize Baker's Law of Cyber Security, which is our security sucks, but so does theirs. And we can find them and attribute this. And attribution will get easier. It's harder and harder to be anonymous, really anonymous on the internet. And as attribution gets better, we need to start working on the question of deterrence. And I don't mean you'd have to drone people.

The indictments of Iranian and Chinese Nationals was a form of public humiliation for those folks, and maybe more for the individuals. We have a set of sanctions that the US Government has never used, which it proposes to use if it can identify acts of cyberespionage for commercial purposes. I think every finance ministry in the world should believe that there should be international financial sanctions on countries that attack the financial system, because nobody wants to see a collapse as a result of a cyberattack. So there are a whole bunch of deterrents options that we should be pursuing as attribution gets better, as I think it is.

MR. SANGER: Chami, is --

MS. CHAKRABARTI: Just briefly, I think the gentleman makes a really, really thought-provoking point. How do we conceptualize this online world? Do we have an arms race online, with the language of offense, and defense, and deterrence, and so on, or do we go through sort of an alternative concept of, you know, of the international space, whose neutrality, and safety, and security we protect in this lovely cooperative way, in a space, the final frontier.

MR. BAKER: They don't call it the tragedy of the commons for nothing.

(Laughter)

MS. CHAKRABARTI: As I recall, Star Trek, it all got pretty nasty pretty quickly, but it's sad. It's sad to think that they'll just be a new arms race online.

There's already a new arms race online, and not, you know, Tim Berners-Lee's great vision.

MR. SANGER: And not just online. Yeah. Okay. Ma'am?

MS. GREWY: Barbara Grewy (phonetic). So is the concept of privacy, or should I say privacy --

MS. CHAKRABARTI: Whichever you'd like.

MS. GREWY: -- actually extinct. I mean with all the data and information that people are voluntarily giving out, and all of the information that we not necessarily intentionally, but because we check the box that gives away all of our privacy, and gives the data of everyone, and all that's been stolen, I mean the amount that is still private, so small, I mean I wonder whether in the future school children, if they want to know about privacy, are going to have to go to an exhibit at the British Museum or the Smithsonian. And a corollary of that concept is, can you talk about how rationale or irrational it is that people were concerned about metadata being taken from phone calls or other communications that was not personally identifiable, and done to keep you safe, but they don't care when Amazon, Google, and all these commercial entities take all kinds of information that goes to your intent and what you're up to, and solely for commercial purposes. So why can you have that dichotomy?

MS. CHAKRABARTI: I would say that -- two fantastic points. Firstly, I would say that privacy is not dead, because it is, in part, just a perennial human craving, just like security. So it's in flux, particularly in this particular moment, where the technologies moved the pace, and the knowledge of it, and the ethics of it, and the politics, and all of it have not yet caught up. So we've got an experimental moment. And there will be some, to use not my favorite American term, collateral damage in the process. But in the end, as with the printing press, you know, we will, you know, I would

compare the internet to the printing press, in terms of the level of innovation. We will catch up. But the privacy, some degree of privacy is just a basic human craving, and it will never, it will never go away, even if we're going through a period where it's been compromised. I think we will catch up with the technology.

Now it can't be an absolute right, of course not, but it never was. The question is where will the balance be struck, and will people, you know, will people be smart about their own privacy and about their relationship with other players, the government, the corporates.

The second point then, I don't think this divide between state, and non-state, and corporate actors is desperately helpful any more. Frankly, what Edward Snowden revealed, governments can cooperate with corporates, governments will contract with corporates, governments will legislate against, you know, it's about data, and it's about when it is necessary and proportionate to invade people's privacy, and who's doing it is largely irrelevant. But you're quite right, you know, people will, to date, and I think it will change, which is why the Apples, et cetera, are so nervous, will trust this cool technology, and Apple, and Google, and so on, more than they will instinctively trust state powers. But that won't necessarily continue, which is why the corporates are all feeling so nervous about this contemporary --

MR. BAKER: We may agree on a big chunk of that. Privacy and the desire for privacy is profoundly human, but the fact is we take our privacy where we can get it. The people who lived in this room, who are in that picture over there, could not have a conversation that was truly private. Strangers could walk in at any moment and then gossip about what was being said over the back fence with other servants. And the notion that you have privacy is an artifact of the modern middle class. That's a new privacy we have. I've discovered, as many of the people in this room have discovered, in the last 15 years making

a phone call to somebody is an invasion of their privacy. You kind of have to apologize for not texting first. And that technology has made it possible to feel that as a privacy invasion. But how do you decide what is private and what is not? It's based in the real world. And Ben Franklin, one of my favorite sages, said on this, "Three can keep a secret if two of them are dead."

(Laughter)

MR. BAKER: And all of us learned about the third grade, when we told somebody who we really liked, you know, in that way, and they immediately told them, that once you've given your secret to someone, it's gone, and you no longer control it. And when we give our information to anybody, including Amazon or Google, it is gone in a way that sooner or later will bite us, and we will stop feeling that it's quite as private as it used to be, just as our kids are already discovering that their location is never private.

MR. SANGER: Okay. So we have for, I think, one more. I agree with you. The difference is you sign terms of service, which you may never read --

MR. BAKER: Right.

MR. SANGER: -- with Google and with Microsoft, you don't really sign those with the NSA and GCHQ.

MR. BAKER: It's called the Constitution.

MR. SANGER: That's right. Let's see, there was another hand out here someplace.

MS. CHAKRABARTI: That's a really broad and blank (inaudible).

(Laughter)

MR. SANGER: One or the other. Was there any last question? I thought I saw a hand before, but maybe

people have decided that we are the last thing between them and the bar, and they have wisely concluded --

MS. CHAKRABARTI: Where the truly private conversations will take place.

MR. SANGER: Yes.

MR. BAKER: And, and where you can drink to forget the likelihood of cyberwar.

(LAUGHTER)

MR. SANGER: That's right. Okay. Well, if there are no more, I want to thank both of you for a very enlightening conversation, and thank you, Clark, for getting us all back together. Thanks very much.

MS. CHAKRABARTI: Thank you.

(Applause)

* * * * *