THE BROOKINGS INSTITUTION

THE FUTURE OF GLOBAL TECHNOLOGY, PRIVACY, AND REGULATION

Washington, D.C.

Tuesday, June 24, 2014

Introduction and Moderator:

CAMERON KERRY
Ann R. and Andrew H. Tisch Distinguished Visiting Fellow
The Brookings Institution

Featured Speaker:

BRAD SMITH
Executive Vice President and General Counsel
Microsoft

* * * * *

P R O C E E D I N G S

MR. KERRY: Well, good morning. I'm Cameron Kerry. I'm the Sara and Andrew Tisch Distinguished Visiting Fellow here at the Brookings Institution. It's a pleasure to welcome all of you and to welcome Brad Smith. So before we begin, let me ask you to mute your cell phones. Don't turn them off because we encourage you to tweet this at the hashtag #techprivacy.

So for the format, Brad will give a few opening remarks. We'll then have a conversation, and we'll then open it up to questions from all of you, so get ready.

Ben Heineman, the longtime general counsel of General Electric, a major American brand, wrote an article for Harvard Law School describing what he called the ideal of the modern general counsel. And he described that as a lawyer statesman who is an acute lawyer, a wise counselor, and company leader who exercises leadership or shared responsibility not just for legal affairs, but for positions on ethics, regulation, public policy, communications, and corporate citizenship. I don't know anybody who fits that description of a general counsel as much as Brad Smith. He has been the general counsel of Microsoft since 2002, joined the company in 1993. Last year when the President met with people from the tech community to talk about the reactions to the Snowden affair along with the many chief executives, Brad Smith was there. He has testified before Congress. He has been involved in a range of issues from competition to the protection of intellectual property to, of course, the issues of surveillance and of rebuilding trust. I tell you that he is a vigorous advocate for Microsoft's positions. I've certainly, at times when I was in government, gotten an earful from him. But he has been engaged in all of that range of issues that Ben Heineman described. He has been Microsoft's voice on public policy issues. He leads Microsoft's efforts on corporate responsibility and community engagement as well.

So it's a real pleasure to welcome Brad here this morning to talk about the broad and difficult issues that we face in this space today. So, Brad, thank you very

much for being here.

MR. SMITH: Well, thank you. It's a real pleasure for me to be here. It's always a pleasure to be here at Brookings, certainly to join Cam -- when Cam asked me to come I said the answer's yes, now what's the question? -- and to join Darrell West and others. There are just so many good things that happen here.

I'm looking forward to talking about an issue that I think is quite important to the future of technology and the future of the country and the future of the world. And I think it's especially important to bring this issue even more to Washington because it is an issue that ironically today is getting more attention in some other national capitals than it is getting here, even though so much of the focus is about the policies and actions of the United States government. But I want to address not only the issues that are important to the government when it comes to privacy, but the companies as well because it is a broad issue.

If I start with where we are today as we look towards the closing days of June and think about the year that we're just finishing, the image that comes to mind is this one: It has been an extraordinary year. It's been an extraordinary year because it was on the 6th of June last year that the first documents were published in *The Guardian* from this gentleman, Edward Snowden, a person who obviously has become literally a household name in many countries around the world.

While the debate has been prominent and it has been pronounced, I think it would be a mistake to link it all to the disclosure of these documents because from any broad perspective, the debate that we are having today about privacy as it applies to governments and even to companies is not only important and necessary, I would even go as far as to say it was inevitable.

If you look from a broader historical perspective -- and I think that is the right place to start -- one sees that this kind of debate has taken place repeatedly in American history. There was a time in the Napoleonic War when President Adams led

the effort and supported the work of Congress to enact the Alien and Sedition Act, and freedom of expression was reduced, but then there was a broader debate that followed. Similarly, President Lincoln suspended the writ of habeas corpus during the Civil War. President Roosevelt interned Japanese Americans solely because they were Japanese American. And there have been, therefore, multiple times in the nation's history when steps were taken in a moment of crisis to protect the public safety. But ultimately when the moment has passed, the question has always arisen. Where should the pendulum rest once that moment has come to an end?

That is the question before us today. As we look past the horrific events of 9/11, we need to look forward and ask ourselves how do we want the balance to be struck for the longer term for our country? I think when you think about the longer term, it makes sense to start in many respects where our country began and think hard about the values that have been at the bedrock of our society—literally—since the 1700s.

It was in this building that you see here in Philadelphia, Independence Hall, where as virtually every American who made it through high school will recall that it was on the 2nd of July, 1776, that the colonies voted for their independence. And then it was two days later on the 4th of July when the founders signed the Declaration.

But I think it's interesting today to reflect on what happened the day in-between, the day no one talks about. After all, why should they? The 3rd of July, 1776. It was on that morning that this person, John Adams, got up and before going over to Independence Hall he sat down and he wrote a letter to his wife, Abigail, who was back in Boston. And he used that letter to reflect on what he thought had started it all, the seminal event that had led to the American Revolution. And in his mind, throughout his life, he always traced that seminal event to this building, the State House in Boston, and he traced it to a specific case that was argued in 1761 in the painting that captured this case that was created later. It was a case that was argued by James Otis and it was all about one issue. It was about the ability of the British government to use what was called

a general warrant or as some called it a writ of assistance and go from house to house to house to look for customs violations without any probable cause that there was any evidence of a crime committed within.

Interestingly, this was an issue on both sides of the Atlantic. James Otis argued it in Boston in 1761. A member of parliament, John Wilkes, argued it successfully in London just a year later. And on both sides of the Atlantic the argument was made that this kind of governmental ability, to enter a premise without any particular probable cause about evidence of a crime within, was a fundamental violation of civil liberties. And John Adams, as it turned out, when this case was argued in 1761, was a young man 25 years old studying to become a lawyer who sat in the audience. And he would always say to the day he died that it was that case, that courtroom, that day, and this issue that set this country on a course for independence.

Now, it was 13 years after the Declaration of Independence was signed that in many ways that principle was fully realized. It was in a different building. It was on the corner of Wall Street and Nassau Street in Manhattan. And the building that stood there then is not the building that stands there now. It was this building. It was the first Capitol of the new government after the completion of the new Constitution, and it was in this room where the first House of Representatives met. And it just so happens that it was 225 years ago this month on the 8th of June that James Madison stood up for the entire day and introduced and defended the concept of having a Bill of Rights. As anybody who knows history will appreciate that even when James Madison stood up, he was not necessarily the tallest person in the room, but he commanded the respect of everyone's ear. And as the afternoon wore on, people challenged him as to why a Bill of Rights was needed. After all, Madison had not been an early proponent. And interestingly, he took people back to that case in Boston. He explained that a government that had the authority to protect public safety, that had the authority to collect revenue, that had the authority under the Constitution to do everything that was

necessary and proper to fulfill those responsibilities, also needed to have limits. And one of the limits he pointed out was the need for what became the Fourth Amendment, the right of the people to be secure in their persons, houses, papers, and effects from unreasonable search and seizure. And in particular, as the Fourth Amendment calls out, it was made clear that there would never be a general warrant in the United States because the government could get a warrant only based on probable cause and only by satisfying with particularity a belief that there was evidence of criminal activity within a specific premise.

Now, ever since that time, technology has advanced and we have lived under the protection of the Fourth Amendment. Benjamin Franklin invented the postal system. Criminals invented what became known as mail fraud. And even though people took their private communications and it left their house; in fact, they literally gave it to the government. That's what people do when you send something through the mail. The courts held that the Fourth Amendment applied and people had a reasonable expectation of privacy of what was in a sealed envelope. Similarly, Thomas Morrison created in effect the software for the telegraph. The telegraph exploded. Criminals invented wire fraud. The government had to investigate it and yet the Fourth Amendment continued to apply.

As soon as the computer and the Internet were invented, Internet fraud was certain to follow. And the fundamental question, certainly one of the fundamental questions for our day, is what the Fourth Amendment will mean in this new Internet Age.

Ultimately as we think about these questions, we need to think about the three goals that clearly are important. It is, of course, right and proper to say that public safety, the protection of our country, remains a paramount concern for our government. It is and always will be just as it has been in the past. This is certainly an issue that we appreciate acutely at Microsoft. We, perhaps more so than any company in the tech sector, have invested in a digital crimes unit that works with law enforcement to protect

children, to protect senior citizens, to protect consumers not just in this country, but around the world from fraud and malware and other threats to public safety.

We can't talk about government surveillance without starting by acknowledging that we must continue to protect the public, but equally there are other goals as well. We need to ensure that the fundamental freedoms enshrined in the Bill of Rights retain the type of meaning in the 21st century that they had in the centuries that preceded us.

And third, we need to think about technology as well. As a company, Microsoft played one of the more unique roles in taking an invention that looked like this -- it was bigger than a house; it wouldn't even fit in this room -- and instead turned it into something that a young Bill Gates could dream would literally become a device that would be at every desk and in every home.

And in doing that it was about much more than making these devices smaller. This device was given a name and it was given a name for a reason. It was the personal computer. It was about democratizing technology. It was about creating a tool that everybody could use to make their lives better. But, of course, as people moved their private information from their desk drawer to their desk top, it was also abundantly clear that people needed to trust this technology as well. People will use technology only if they trust it. And as we now live in an era where data is moving from the desk top to the data center and the cloud, we need to find a way that protects public safety, preserves our fundamental freedoms, and promotes trust in this technology all at the same time. I believe that if we put our minds to it, that is an achievable goal.

It's certainly something that we've been thinking about at Microsoft for some time. People often ask us well, did we really just start to focus on this hard after the Snowden documents were disclosed? And the answer, of course, is no. We experienced these issues shortly after 9/11 as did the entire country. Some of this actually came to light in an article that *The Guardian* published last July. It covered a

specific document that was leaked from the NSA. It's a document that summarized a report of the Inspector General. It talked about a voluntary program where the NSA had gone out to telephone and Internet companies and asked them voluntarily to provide access in bulk to a lot of communications content, including email.

And interestingly, the IG's report does not name names in terms of companies, but it talks about a number of companies. They're called companies A through H. One of the companies that got our attention when we read the document was company F. It turns out that if you read this document, it says that in October of 2002 the NSA talked with people from the company's department of legal and corporate affairs. I can tell you that today in the tech sector, there are several companies that have departments of legal and corporate affairs. But I can also tell you that in October of 2002 there is only one tech company that I know of that had a department with that name. It was Microsoft. And if you read the rest of the report it says that the NSA asked company F to turn over in bulk email content and that company F said no.

We thought hard about how to deal with the question that had arisen. I still remember meeting with Steve Ballmer, our CEO, in the fall of 2002. I remember, in fact, talking about John Adams and Abraham Lincoln and Franklin Roosevelt and how the decisions we would make would need to stand the test of time. They would need to be the right decisions for the moment, but they would need to be the right decisions when the moment passed, because it was clear that it would.

And fundamentally what we came to was what we felt was the right principled approach; that the only basis on which it made sense for us to turn over the private communications of our customers to any government in the world, including our own, was pursuant to the rule of law and pursuant to legal process. After all, no one had elected us. If the United States government felt that it had a need for the private communications of our customers, it should turn to legal process. And if it felt that legal process didn't go far enough, it shouldn't ask us for help. It should turn to Congress

because that is the way that the fundamental rights of citizens should be protected and regulated in a democratic society. And I continue to believe that that principle above all has served us well in the past and will continue to serve us well in the future.

That's one of the reasons last summer we sued the government. We started to read these stories in *The Guardian* and elsewhere that talked about the government's access to massive amounts of data, and yet we knew that we had not turned any data over voluntarily and we knew what we had turned over pursuant to legal process and it was a relatively small amount of information. And we had a hard time reconciling these public reports of government access to large amounts of data with the relatively small amounts that we knew had been provided.

In a sense the answer that unlocks the riddle was provided by Bart Gellman of the *Washington Post* in this story on the 30th of October last year. The *Post* reported that the NSA, either by itself or in collaboration with another government acting outside United States territory, had tapped into the data centers or cables of Google and Yahoo! And there was no report about Microsoft, but we had to assume that if the government was interested in some companies and had managed to get access to data in some companies without them knowing, that it might well have done so for other companies as well.

And that continues to be a factor that has fundamentally influenced the way the entire tech sector looks at all of these issues today. We knew what we were being asked to do. We knew what we were being required to do. We didn't know what was being done without our knowledge. And we still do not know all of that even today.

It led Microsoft and indeed many other companies to take a number of new steps. We encrypted more data, basically the data for all of our services. We took new steps to promote transparency and to increase contractual protection for our customers. I will say I do believe that President Obama took an important first step when he gave his speech at the Justice Department in January of this year. It was a first step.

It was an important step, but fundamentally we need more steps to follow. But the President framed the issue correctly in my opinion. He fundamentally said that this is about how we in the 21st century continue to protect the public safety and hold true to the fundamental values of our country and the Constitution.

And there have been some additional steps that have followed. The government settled the case that we and Google and others had filed so that we could publish more information and on the 3rd of February we did that. And we showed that in the six-month period that was covered in the first report, we had responded to fewer than 1,000 FISA orders and those orders had covered less than 16,000 user accounts. That was a good step, but more steps are needed.

We do need Congress, in my opinion, to close the door on unfettered bulk collection of data. The House got us close, and we should all hope that the Senate can get us the rest of the way so that the public here and around the world can have the fundamental trust it deserves in the technology it uses every day. That is a first step.

I think another step that we need to focus more on is the role and nature and proceedings of the FISA court. I think it's important to step back and remind ourselves of what an unusual court this is when you compare it to the tradition of American jurisprudence. This is a court that meets in secret, not a public court that deals with specific documents under seal. This is a court that has only 15 judges that are appointed by one person, the Chief Justice of the United States. Every one of those judges, of course, was first confirmed by the Senate as a district judge, but this is not the way that cases are typically handled in our country. This is a court that does not publicly publish its opinions. It's a court that creates law that the American public is not permitted to read. And perhaps most importantly, this is a court unlike other courts in our history or today in which only one side gets to tell its story.

If there is one fundamental principle that has been used to ensure that American courts not only act pursuant to the law, but pursue results that promote justice,

it is the adversary system. It's a system that lets lawyers for two sides argue their case. The adversary system is missing before this court. The President has proposed certain steps to create an advocate, but even that small step has not yet been embraced by Congress. And, of course, as we found when we brought our law suit against the government, a law suit that went before the FISA court, it's hard to be a litigant before this court. Anyone who's ever wanted to be a lawyer, met a lawyer, or seen a lawyer on TV, can imagine what it is like to be a lawyer when you receive a brief from the government that has a page that looks like this.

This is not the type of approach that is likely to promote justice, and yet I will point out that the irony is that companies like ours are required to have lawyers with the highest levels of national security clearance so we can comply with the court's orders. And yet, if we have the security clearance needed to read the orders and comply with them, do we not deserve at least the right to read what the government is arguing when it is litigating against us? There is more room for more discussion about more reform.

I think another step that we in our industry continue to look for is the assurance that our Constitution and the Fourth Amendment will apply to us as American citizens and American companies even when we're outside the United States. We do not believe that the United States government should hack into the data centers of United States companies outside the rule of law. We deserve, as the courts have recognized not only over the decades, but centuries, that we continue to benefit from the protection of the Fourth Amendment even when we are abroad.

And finally there's one other issue that has assumed growing importance that deserves more attention here in Washington. It is the issue that when I was in Berlin last month everybody wanted to talk about. It's about the geographic scope of warrants today that are pursued by the United States government. Because what the U.S. government has been doing is serving warrants on companies like Microsoft that have data centers and they're giving us an account name. And they are telling us to go from

building to building to building and from state to state to state and even from country to country to country if that's what it takes to pull all of the information that belongs to that customer and turn it over to the government. If you think back to the general warrant to which James Otis objected in 1761, this is a warrant that would have made the British blush because it so much farther sweeping in its scope.

And there are some who say but it's a new day. People are no longer keeping their information in their house. It's unduly burdensome to expect the government to know where people actually have information and plead with particularity as the Constitution requires where someone should pursue a search. But I think it's worth reflecting on the fact that this is not a new problem, it is not a new issue, and it's not an unsolvable problem either.

This problem actually was created in 1886 when a gentleman named Henry Brown filed for the first patent application for the safety deposit box. It was at that point that people actually started moving some very valuable papers out of their homes and into banks. And, of course, banks started out small, but security deposit boxes started to spread and banks today are major institutions. Look how many branches Citibank has on the island of Manhattan where the first Congress met. Look at the number of locations around the world where Citibank has branches. And yet since 1886 and to this day it is accepted by law enforcement and the courts alike that the government cannot serve a warrant on Citibank and give the name of a customer and tell Citibank to be its deputy and search all of its branches for any safe deposit box that customer might have. Instead the government must do some legwork. It must pursue an investigation, and it must plead, with particularity, the branch where the safety deposit box exists to which the warrant applies.

If this has been a solvable problem since the 1880s, I think we have to ask ourselves if there isn't a better way to solve in the year 2014 than by deputizing technology companies and telling them to look literally everywhere on the planet,

because in this case there is a case that does reach that far.

It's a question that fundamentally raises issues of trust, not just for American citizens, but for citizens around the world. That's why we at Microsoft have challenged a warrant that the government has issued, a warrant that is now being litigated in federal court in Manhattan. In this case there's not only the question of the generalized nature of the warrant, but it's fundamentally a question of how the world is going to work. Are governments going to think about each other's borders or are they literally going to reach as far as they can based on the nationality of their data center providers anywhere that they want? Because in this case, when we found out who the customer was, we found that it was a customer that was from Europe. And we found that the data center in which this customer's data resides is not in the United States. It's on this island. It's in the Republic of Ireland. It's in this town west of Dublin. It's down the street from this little corner, and it is in this building -- a Microsoft data center.

And, hence, we have objected. We've pointed out that under the Electronic Communications Privacy Act Congress did not give the United States government the authority to execute warrants outside the United States. It did not give the government the authority to ask tech companies to literally break down the digital doors of their facilities and go look at what was inside and turn it over to the government.

Ultimately, we think it's important to recognize this is Ireland. It is not Iran. This is a country that has a close relationship with the United States. This is a democracy that protects the rights of its people. If the U.S. government is going to seek to reach into Ireland unilaterally, on what basis can the United States government possibly stand up and object when other governments seek to reach into data centers that are here in the United States? Ultimately, in the short term, people may think that this is about protecting the rights of the American public by giving law enforcement access to information elsewhere, but it is every bit as much about protecting the rights of Americans. If we want to protect the rights of Americans for data that exists in the United

States, we as a country need to pursue principles that can be applied across the board.

And, hence, we believe that we need to turn to the courts. We need to rely in this instance on the Mutual Legal Assistance Treaty that exists between the United States and Ireland. This is not an old treaty written in the 1800s. This is a treaty that was written after 9/11. It's a treaty that creates the basis for fast and efficient cooperation between law enforcement agencies and the courts in our two countries.

And ultimately we need to look for better solutions. Yes, there are times when law enforcement in one country will need access to data that's held in the data center in another country, but it should look in the first instance for opportunities to do this in a collaborative way with our allies. And it should do it under principles that ensure that even if the U.S. government does act unilaterally, there are limiting norms that people can understand and respect both under U.S. constitutional principles and under the kinds of norms that can genuinely exist on a worldwide basis.

Ultimately, I think it's worth stepping back and reflecting on the nature of the discussion that literally is sweeping around the world when it comes to privacy. Here in the United States, the forefront of this discussion has been about what is fundamentally the relationship between governments and citizens all around surveillance. Interestingly in Europe over the last 20 years, there has also been a vibrant debate. It has tended to focus not so much on government, but on companies and the degree to which companies access data and how they use data from consumers.

In effect, I believe that these are two halves of a common whole because there is one word that applies to both citizens and consumers; they're called people. And what we're fundamentally talking about is the rights of people to be secure when it comes to their personal information in the 21st century. And we need to recognize, as an industry I believe, that the tools that we are creating are wonderfully beneficial in so many ways, but as we've all come to appreciate, they collect and share an enormous amount of information.

From time to time we read in the press that a court has issued an order in a criminal case requiring someone to wear an ankle bracelet. What does an ankle bracelet show? Just shows where somebody is located. Without any court order, millions of Americans every day carry in their pocket or their purse a device that shows their location every moment of the day. It records what people write. It records what people read. These are fundamentally beneficial instruments of technology and yet if we don't think about the broader implications of what we are creating, we will put people's fundamental privacy needs at risk.

Of course, there are people who ask does any of this matter? We have new technology. Maybe the new generation really doesn't care about privacy anymore. They just care about using the technology. I think it's worth reflecting first on the fact that it is technology that fundamentally unleashed the whole privacy debate in the first place. It was Louis Brandeis before he went on the Supreme Court when he was at Harvard Law School who coined the phrase "the right to be let alone." It was in a *Law Review* article. And what I think is worth reminding ourselves is that that phrase appears at the end of a paragraph in that *Law Review* story, but the first sentence in that paragraph talks not about the law, but it talks about technology. It was the camera, another invention that everybody loved that suddenly exposed people when they stepped out of their front door to being photographed perhaps with someone with whom they really didn't want to be seen, and it was that that started this debate.

Of course, in this day and age people say that was then, this is now, people don't care anymore. Just look at Facebook, they say. Privacy must not matter, look at Facebook. I remember the day in April of 2007 when we at Microsoft made an investment in Facebook. When we made that investment, Facebook had 25 million users. The most interesting thing about Facebook at that point was that it was not the market leader. The market leader was Myspace. Myspace had over 100 million users. If you look at the history of technology and ask yourself how often does a company that is

well behind the market leader -- when the market leader hits 100 million users, how often does that company come from behind and assume the leadership position? The answer is very rarely. And yet as we all know, look what happened in the years after -- Myspace stagnated, Facebook took off. Why did this happen? Well, interestingly, part of the reason is captured in a book by David Kirkpatrick, a technology writer, who points out that by default when you shared information on Myspace, it was accessible to the entire world. But by default when you shared information on Facebook, it was only accessible to your friends and people in a particular network. So as he points out, there was a degree of privacy built into Facebook that wasn't present in Myspace. Perhaps people do care about privacy, but perhaps they've redefined the term.

That is what I believe has happened because what we're seeing today is that consumers want to share their personal information, but -- and there's two big buts -- they actually want to decide who they share that information with and they want to determine how this information will be used. If you ask people not just here in the United States but around the world whether they actually recognize this phenomenon, one thing I have found that is universal is any parent who has or has had teenage children in the last ten years knows what this is talking about. I personally negotiated the first industry privacy agreement with the Federal Trade Commission over privacy in 2002. That negotiation was easy compared to the negotiation I had when our daughter was 15 and my request was that she friend me on Facebook. Even kids, who want to share a lot, don't necessarily want to share everything with their parents. And, of course, any of us who can remember what it was like to be a teenager probably needs to acknowledge that this was true in the past as well. It's just the technology that has changed.

Interestingly, I think Sonia Sotomayor captured this remarkably well in a short concurring opinion in 2012 in a case called U.S. v. Jones that came out of San Diego. Historically, she pointed out that in the United States fundamentally when people talked about keeping information private, what they meant was keeping it secret. People

no longer care about keeping information secret to the same degree, but that doesn't mean that they care less about being able to manage who accesses their information and how they use it. That's the new definition of privacy.

And, in fact, this is continuing to evolve with new technologies as they come forward. If you consider not just Facebook but Snapchat, you see it yet again. Here is a technology that fundamentally has been driven by middle schoolers, it's young teenagers. And it was interesting when the CEO -- the 23-year-old CEO -- of Snapchat, Evan Spiegel, spoke about this in Los Angeles earlier this year. He took that phrase "personal computing" and he talked about Snapchat as "more personal computing." What he fundamentally talked about was what he called the notion of content being ephemeral.

The thing that is fascinating to those of us who were part of the Microsoft case with the Justice Department over antitrust issues in the late nineties was when people started taking email. We note the fact that it was often quoted out of context. People didn't have the context that they had if you were talking to somebody at the proverbial water cooler. And yet what Evan Spiegel pointed out was that the beauty of Snapchat, because you see a photo and then it is designed to disappear, was that it had this ephemeral nature. And as he said, it's a conservative idea -- the natural response to radical transparency. He said that it would mirror the expectations we have when we're talking in person, that it would restore integrity and context to conversation. What I think is most interesting about this is that he never once used the word privacy. His generation doesn't necessarily use the word, but they talk about the concept of controlling how their information and their content is shared.

And ultimately you can think about this not only from the perspective of Facebook and Snapchat in our industry, you can think about it from the perspective of another group of people whose business is to respond to the concerns of the public: elected officials. Look at the wave of legislation across the United States and look at

where it always starts, the states, and look at the state where it starts first, oftentimes that's California. Last year there were 33 privacy bills introduced in California. We are seeing state after state take up this issue.

And, of course, we're seeing it not just in the United States. We're seeing it around the world, and look at this graph and how the number of countries that have privacy laws continues to grow. Fundamentally, this is an issue that will continue to become more important because right now if you look at the world, there are 1 billion personal computers. There are 2 billion Smartphones. There are 7 billion people. And by the end of this decade, there will be 50 billion devices in the Internet of things connected to data centers around the world. We will enter a world where every thermostat, smoke detector, fire extinguisher, parking meter, traffic light, garbage can, and you name it, is a connected device. This issue is going to become more important, not less.

Ultimately, I think what we need to consider is how the two halves of this issue may come together. I believe the questions are the same, but the answers may differ. But if we think about the relationship between citizens and the government and consumers and companies, there are four things that we will need to grapple with. First, how do we ensure transparency? How do we ensure that people have a right to know in an appropriate way what governments and companies are doing?

Second, how do we ensure the public has appropriate control over personal information? Of course, individual citizens don't have the right to determine whether they're investigated by the government. But the public as a whole absolutely in any democratic society should have the right to control what the government does through the rule of law. And similarly, I believe that consumers should have the right to determine how their information is used by companies through appropriate notice and consent and management of the use of information.

Third, how do we ensure accountability? In the government context, the

Executive Branch needs to be accountable to the courts. That's why the issue of FISA court reform remains so important. When it comes to companies, I believe that companies do need to be accountable to regulators through regulation. It needs to be well-designed regulation. It needs to be thoughtful. It needs to be balanced. But we cannot live in the Wild West when we're talking about information that is this important to people.

And finally, how do we ensure international norms and collaboration so information can cross borders when it should? These are the four questions that we will need to grapple with in capital after capital around the world.

In closing, I would say this. Technology is a tool. It is a tool that, at its best, empowers people. It is a tool that needs to serve people; equally governments exist to serve people. We need to come together. We need to ensure that important issues of public safety are addressed, but we need to do so in a way that ensures, as well, that technology in the 21st century continues to serve people. That's what this conversation is all about. Thank you very much.

MR. KERRY: So, Brad, thank you. Thank you for particularly, I think, sketching out the world that devices and data are leading us to and the explosion that we're seeing in the collection of data and the management of data. We are sort of at a hockey stick adjusted to the beginning of that curve in terms of the volume of data that's being collected.

So let me pick up with your four questions and some of the points that you see in common between the private sector side and the government. I thought your four questions maybe you were going to start with was why is this day different from all others. I guess, frankly, that's why we have you here.

So you talked about control. You talked about transparency. You talked about accountability. You talked about international collaboration. And certainly, to me those sound very familiar from the 2012 White House blueprint, the Consumer Privacy

Bill of Rights. What do you see as the shape of regulation? The Fidessa report reaffirmed those principles after some process. The administration should send something up to Congress. What should that look like?

MR. SMITH: Well, first of all, I think and I hope that the administration will send something to Congress. I mean we went on the record. I gave a speech in 2005, endorsing national privacy legislation in this country. I think it's long overdue at this point. It is unusual for Americans to look across the Atlantic and at least publicly find anything they like in Europe, but the Europeans have been at this basically since the eighties. And there are certain principles that have become global, I believe. And they're not only reflected in European law, some of these are reflected in sort of fair information practices that have been accepted by industry and others.

I do believe that people have a right to know how their information is being used. So I think that having transparency obligations that apply in different settings makes sense. I actually think this is an area where we as an industry need to work harder; certainly we as a company need to take more steps than we've taken so far. We're focused on that.

I believe that the whole system of sort of notifying people and asking for their consent before information is shared and used is under stress, just because frankly people are asked so often during a month to sort of click on something and so everybody clicks on it without reading it. But I don't think that means we should throw that principle overboard. We need to think about how the public has the right to know and consent to the use of its data and make that work in the 21st century.

I think that there are broad practices that amount to good information practices about how companies should use data, how they shouldn't use data, and how they should be accountable if they lose data or if there's a data breach. I think that should be addressed as well. I mean we do have some important building blocks in the United States under HIPAA. We've got health care data under Gramm-Leach-Bliley.

We've got banking data. It's just that in the United States at the national or the federal level this has grown up in silos and it's time to take the parts of the silos that work and generalize it.

MR. KERRY: So you talked about international collaboration and mentioned Europe. If you recall, part of the genesis of asking you to come here was that a few months ago Microsoft went to European privacy regulators and got approval of some of its standard contract clauses. You've spent a lot of time in Europe dealing with some of the fallout of the Snowden affair and how to rebuild trust.

So, talk a little bit about how we do that in Europe, how companies can build that trust, and more especially, how do build bridges? How do we deal with some of the differences that exist and allow for those, but still be able to move data around the world in ways that in this global economy we need to?

MR. SMITH: It's a great question. I think anytime you want to build a bridge, at least politically or metaphorically, you have to start by understanding how people think on the other side of the canyon. It doesn't mean you have to agree with them, but if you can't understand what they're thinking about you're never going to build a bridge.

And I think what that means for people in Washington is first, really understanding the different cultural norms that people are considering in some other countries around the world. The single place where this privacy issue is probably the hottest, at least in June, is Berlin. And you can't go to Berlin and talk about data privacy without quickly appreciating that this is perhaps the only country in the world where there are people who are alive today who experienced the abuse of data first by the Nazis and then by the Stasi. And, of course, if you lived under those kinds of regimes and you saw how a government used information -- not necessarily to protect the public, but the regime itself -- you'd come to appreciate where they're coming from and it's a different past that what we experienced.

One of the things that we have to also appreciate in every country is most of the time people are willing to have a level of confidence in their own government that they don't extend to other governments. So even when we believe that our government is acting not only to protect the safety of Americans, but say the safety of Europeans, the Europeans say we elect our own government. We'll look to our government to protect us. We're not willing to give another government that same level of confidence, and we're not going to do that for any government either.

So I think it starts by understanding, frankly, that this is an issue that is thought about differently. We should not in my view attempt to apply the same law in every place. We shouldn't take European law and just copy it for the United States. And we shouldn't expect to take U.S. law and copy it in Europe or anywhere else. But we are going to need to build some bridges using some principles that are perhaps more global.

MR. KERRY: So, in this global economy, you talked about having data in a data center in Ireland and about the case that Microsoft has where you're resisting extraterritorial application of U.S. access to records. Different companies have taken different positions in terms of what matters. Is it where the data center is? Is it where the citizen is? And if I understand correctly, it is your position the data is located in Ireland, so that's the key fact in limiting U.S. access. Is that right?

MR. SMITH: I believe under current U.S. laws -- it was written by ECBA -- in that case, yes, and I think more fundamentally, yes, the law applies where the data reside. And I actually think that that is in general a good principle. It doesn't mean that there might not be some exceptions and it's probably worth talking about them, but you might ask why is that a good principle? Well, the reason it's a good principle is it gives us the ability to look at different countries around the world. And if we want to protect data and people from what might be a human rights abuse, we can do that by keeping the data out of that country. We don't put a data center in that country. But the moment a different principle applies, if it's applied without exception, without any limiting principles

at all, you give whatever government you want to pick -- if ISIS takes over a country, are we comfortable saying that they should have access to the data of an Iraqi citizen who lives in the United States because they can? Or are we going to say that they only get to reach data in Iraq? Or are we going to say that governments are going to have to work this out between themselves? I at a minimum think that this is a conversation that needs to happen and not just rely on a principle that governments should be able to go get whatever they can.

MR. KERRY: So let me have a little bit of that conversation and explore some other principles. So what about a drop box? My European cousin shares some photographs on Dropbox and suppose he only shares them in Europe. As far as I know, Dropbox has its data centers in the United States. Would that be available in the United States?

MR. SMITH: Well, under existing law -- and I don't know anything about Dropbox so I will take your premise. Look, if the data is in the United States, it's subject to the reach of U.S. law. I mean everything that's in the United States is subject to the reach of U.S. law; everything in any country is subject to the reach of that country's law. That's both a legal statement and it's a practical statement, and I think that's a principle that people can probably figure out how to live with. And then as I said, you build data centers in countries going in knowing that the data in that data center is going to be subject to the law of that country.

MR. KERRY: So, Brad, what do you say to cynics who look at the position Microsoft's in and say it's easy for Microsoft to locate data centers in Europe or elsewhere, and look at things like that, or look at positions you've taken on regulation or vis-à-vis Europe and say well, that's in your competitive advantage? It's in the company's interest to do that in relation to other players in the marketplace who don't have the same scale or don't have the same business plan.

MR. SMITH: Well, it's a fair question, it's a good question. And I think

fundamentally you're asking hey, do you believe in what you believe because you believe in it, or do you believe in it because you think you're going to benefit from it? Well, first of all, I think we believe in the things we believe because we really do believe in them. That's first. I mean we believe in personal computing; that's what created us; that's what we've supported; that's what we've advanced with every product that we've created. It's always about trying to ensure that these are tools that empower people. And by the way, if we do a great job of empowering people, if we do a great job of creating technology that people will trust, yeah, we'll hopefully grow. We'll hopefully succeed, and we'll hopefully succeed because we deserve to succeed.

I will hasten to add that ultimately I think on many of these issues this is not going to be something where one company benefits and another company doesn't. I think that technology will rise or fall together. I think that the American IT sector will rise or fall together. And I would also say I would be the first to say that we at Microsoft have a lot of work to do. I mean we had a lot of work to do last December when we said we were going to expand encryption. We got to work to do it. I think we have a lot of work to do to expand transparency for consumers, and we're focused on it.

To me this is ultimately about choosing the principles that we believe in in terms of reconciling the values that are at stake and then getting good at them, but not the other way around, not choosing principles that serve what we happen to be good at today.

MR. KERRY: It does seem to me that witness some of the things that a number of tech companies did together in response to Snowden, everybody's a little bit in the same boat here.

MR. SMITH: I think certainly on the government surveillance issues, our industry is almost entirely united.

MR. KERRY: So you mentioned encryption and I want to ask one specific question and then turn to the audience. You've taken steps to strengthen

encryption. You've also indicated that there are some challenges in doing that and some maybe created by the U.S. government. What do we do to strengthen encryption and to strengthen trust in encryption?

MR. SMITH: Well, the most important thing to do is use stronger encryption and use it across the board, and across the board really means two things: You use it on all of your services that have content, and you use it for both data that is "at rest," meaning it's a file that's stored on a server in a data center, or you use it for data that's "in transit," meaning the data's being transmitted say from one data center to another over a cable or from a data center to a consumer and then it gets decrypted on the user's device.

It's actually expensive. It's required that the industry redeploy resources. It's required that engineers be moved off of projects to go pursue this. It's required that certain aspects of data centers be rearchitected. The fact that the entire industry has stepped up to make this investment basically simultaneously I just think is a reflection that we are in a business that relies on people's trust.

I mean we really are -- look, let's just step back for a moment. It doesn't matter what personal information you have. We're offering a world where you should feel comfortable storing that in the cloud. Of course, there is no physical thing that is a real cloud in which this is stored. What it's really being stored in is a data center. You don't even know where the data center is located, but you need to have confidence that this information is still yours. And, therefore, trust is a prerequisite and encryption is a fundamental part of ensuring people's trust.

MR. KERRY: So your comment about cloud computing not being a physical thing just brings to mind meeting with an official whose leading part of the European review of the data protection regulation and being asked what is this cloud computing?

So let's turn to the audience. We have some questions here. Yes,

ma'am, in the front. Did you have your hand up? Okay, so we've got a microphone coming to you over here.

QUESTIONER: Hello, is this on?

MR. KERRY: It does not sound like it's on.

QUESTIONER: Oh, it says "dead battery" actually.

MR. KERRY: Okay. So for those who couldn't hear, it says "dead battery." Boom it out and --

MR. SMITH: We'll repeat the question.

MR. KERRY: We'll get a new, fresh battery. Could you identify yourself, please?

QUESTIONER: Yes. Hi! I'm Julia Tecona. I'm a doctoral student at the Institute for Advanced Studies in Culture. I'm out of the University of Virginia, and my research is on technology and privacy concerns from a sociological perspective. And I couldn't help but notice how much trust came up in your talk today and in your comments, and I think it's an extremely important aspect of this. But it's also a very complex social and emotional response to these technical issues. And so I'm wondering, we know from sociological research, a lot of which came out of Microsoft's great social media collaborative, that people's trust in these technologies often doesn't come from a sophisticated technical understanding about the processes in which their data is stored and all these different procedures and those privacy notices, but more of a sort of generalized social trust in the company or in other users even. And I'm wondering based on that, what do you see as Microsoft's responsibility to making these processes more understandable and also educating the users about what it is that they're signing up for?

MR. SMITH: I think it's a really important point, and I think there are a couple of dimensions that are worth thinking about it. First, on a sort of a company-by-company basis, I do think we have a need to make things simpler. Software companies are not necessarily great; it's not intuitive necessarily about how to make something as

simple as it might need to be, especially for a consuming public on a national or global basis. So we do need to make things simpler. We need to ensure they're clear, that they're understandable, and that if people do stop and think about these things that they would resonate with the balance that is being struck; that they would agree that the right balance or reasonable balance is being struck.

But I also think that there's a broader dimension of what you're referring to. People really react based on their own individual or broader community or national experience. And you see with a lot of technologies that people have trust until something goes wrong and then all of a sudden things change. And one of the examples that I've always thought is really important for people in the IT sector to think about is the history of the nuclear power industry in the United States and what happened after Three Mile Island. Basically, in the run-up to Three Mile Island, there was not a broad public discussion about nuclear power the way there was in some other countries. People were very comfortable with it, but so comfortable with it that there wasn't as much debate in Congress about it. And then when Three Mile Island happened, the industry died in a day. There has not been a nuclear power plant that's been added since that day, and then you look at other countries where there's been a future for nuclear power.

So for me the lesson is it's actually important to have the conversations with governments, with the public, that people in industry might otherwise want to avoid because it's a difficult topic. But if you can talk about it and build a real consensus, then if something goes wrong, if there's a data breach at a major retailer or something else even worse happens, you have a foundation on which to try to sustain trust through that; hence, this kind of conversation is quite important.

MR. KERRY: So let me take the prerogative to ask a follow-up question.

MR. SMITH: Sure.

MR. KERRY: It strikes me that the way privacy operates today, an awful lot of transparency relies on that sort of notice and consent framework or whatever is said

in the privacy policies upfront. But what's really needed is for people to have a better understanding of what data is collected about them and what picture that data presents. What are the inferences that people can draw from the data? So how do we get there? How do we do that? What's Microsoft doing to provide or educate people about that?

MR. SMITH: I think fundamentally what all of the companies in our industry are going to need to do is build overtime what you might think of as a dashboard that you can go to so you can see the data about you. You get to see what's there. You have the opportunity to look and if some of it is wrong, you have the ability to correct it. You get to see how it's used. And there is some way technologically for people to be able to have a level of control in an appropriate way over how their information is used. I think that that's where we're going to need to go as an industry, and I think that's where -- if you just look at the tide of law and regulation on a global basis and step back from a specific month or year or an individual country, that's sort of where things are pushing. And I think that, on balance, has huge amounts of nuances and technical complexity and all kinds of difficulty and engineers will tear their hair out over this thought, but it's ultimately where we'll need to go in some generalized sense.

MR. KERRY: I saw a question at the back of the room there.

QUESTIONER: Al Brault, Sidley Austin. That was a great speech. Thanks for the real tour de force on development of the privacy law. My question is about your comment on regulation and the need for it. In Europe privacy is considered a fundamental right, but it's subject to a balancing against 51 or 52 other fundamental rights and it's also subject to the principle of proportionality. In the United States, regulation is typically subject to either a formal or informal cost-benefit analysis. But with privacy, like other kind of metaphysical issues, philosophical issues, it's very hard to do a cost-benefit analysis because the benefits are not really tangible. But, nonetheless, if you're going to regulate something, it is going to impose costs, it is going to limit other abuses in economic and other uses. How do we go about really quantifying or at least

characterizing the harms that are related to privacy, either privacy violations, privacy injuries, or what not, so there can be a reasonable balance in regulation?

MR. SMITH: Well, I first think one needs to think about where you do that kind of analysis, and I would point out that there are basically two places. You can do it when you're designing a law or regulation itself and figuring out how you want to strike the balance, or you can do it as the regulation is applied to individual companies or data use. Antitrust law is an area where you sort of apply this economic assessment of costs and benefits under a rule of reason to individualized company conduct. It's actually difficult to apply that in technology in some instances because there's a lack of certainty about how the equation is going to net out.

So my own view is I think it is appropriate for a legislative body or a regulatory agency like the FTC to go through the analysis when it is designing the rules, but to then just have clear rules that can be easily followed by companies without asking companies to ask their own lawyers to do a cost-benefit analysis in order to predict what the regulation is going to mean in the first place.

Now, that sort of then takes you back to your question well, how do you do that analysis in the first place? I'm not going to say I have some magic answer. I will say that if you look at the areas where we have adopted law in the United States -- whether it's around HIPAA or it's around Gramm-Leach-Bliley or even in other areas where we let people have access to information about themselves, consumer credit and the like -- I do think that there are some balances that have been struck from which we can learn and analogize. I do think there's some benefit that can come from building on that learning.

MR. KERRY: Yes, sir?

QUESTIONER: Jon Peha, Carnegie-Mellon University. I understand the safety deposit box analogy. If my papers are in Ireland, I know exactly what that means. When you say email records are in Ireland, I'm not so sure what that means. Those

email records are almost certainly duplicated in multiple places at any given time. They can be moved or copied for performance reasons or to evade law enforcement very quickly and no one will notice. They can be accessed anywhere in the world. If you're going to embed sort of legal access rules based on the location of information, how do we define what location of information means? Can it be done in a way that gives you the protection that you made a very case that we need without making it trivial to evade law enforcement everywhere?

MR. SMITH: Well, I think you raise a really important question and while I would say it's actually not that difficult to know where data is, I don't think that that actually will answer the fundamental question that you're asking. Look, we actually can determine where data exists. We can even determine not just the data center, but ultimately we can determine what server it's on. And you can walk down a row of servers the way you can walk down a row of safety deposit boxes.

But I think that there are two questions that are really critical that come out of what you're pointing to. Number one, why is data in one place versus another? Look, if there's a common practice of moving data around just to evade laws, that's a problem. I'd be the first to acknowledge that. We don't put data in Ireland because we're trying to evade anybody's law. We put data in Ireland to be close to the customer. Anybody who's ever accessed a Website -- or let's just say you're trying to download a file that you stored. Maybe it's photos. Maybe it's a paper. It is still the case that the longer the distance the file has to travel, the longer it is likely to take for the file to get to you. That's what we refer to as latency in the industry. And it may not be a long difference in historical periods of time, but let's be honest. When you're using one of these devices, whatever you want you want it now.

So what we do is we put European data in Europe because it's close to the customer. We're going to put Brazilian data in Brazil because it's close to Brazilians. There are 200 million people in that country who want to have fast access to their data.

And by the way, these are huge capital expenses; hundreds of millions of dollars now to really build out a large data center. So it is not the kind of decision that a company is going to make without really being thoughtful.

Now, I still think that there's another aspect to the question that you raise, which I do understand and I do think this is a direction in which the debate could potentially head. Let's think about a data center in Ireland. Well, let's think about that belonging to an Irish citizen. Should the U.S. government have access to the data of an Irish citizen in Ireland without going through the Mutual Legal Assistance Treaty with the government of Ireland? I think it probably should not; that's what we're arguing. Any more than do you want the government -- pick any government you want. Do you want any government to have access to American data in the United States, the data of an American citizen, without going through the U.S. legal process? I virtually guarantee Americans will say no, we don't want that.

Now, do a different hypothesis: Imagine it's an American citizen who somehow managed to get the data into Ireland. Now, we wouldn't do that under our business norms, but let's imagine that that's the case. Could you get European governments comfortable with an international framework that would say that if Congress wanted to amend ECBA so that a warrant would reach the data of American citizens or an American resident even if the data's in another country, I think you might have the basis to do something there.

I mean ultimately I am not here to argue that law enforcement should be stopped from doing its job in an effective way. I want law enforcement to do its job in an effective way, but pursuant to the rule of law and fundamental principles that we and other societies can look at and say yes, these make sense and we want them to be applied on a reciprocal basis.

And I would hasten to add that if we can't get to this world, then law enforcement is going to have a bleak future anyway, because if we, for example, cannot

get the German government comfortable, they will go forward with a procurement regulation they've already proposed. Their proposal would say that basically you cannot put German public sector data into the data center of an American company. Well, if the data's not in an American company in the first place, U.S. law enforcement isn't going to be able to reach it. So I would argue that the long-term interests of public safety in U.S. law enforcement are only served through an approach that builds a genuine international understanding with which people are comfortable.

MR. KERRY: So let me jump in with a follow up there because I agree with much of what you said. But isn't there a tension between saying that jurisdiction should lie where the data resides and the position of many governments that the Internet should be subject to national jurisdiction and national boundaries? And if we're going to say that where the data is, the national boundaries define that, or does that reinforce sort of that approach to the Internet?

MR. SMITH: In what sense? That you actually do create more national boundaries?

MR. KERRY: That a government -- yeah, that governments define their jurisdiction over the Internet by their national boundaries and if it is within their national boundaries, they control it.

MR. SMITH: Well, I guess the first thing I would say is look, that's the world as it exists today. I mean the notion that people can't -- look, I met some people on the West Coast who would say that no, we created a cyber-world that isn't subject to the laws of any country. I don't recognize that world. It actually doesn't exist. There is no cloud. These are physical facilities. They are data centers, and they absolutely are subject to the laws in which that data center is located. I'm not advocating that as something that should be. I'm just saying that is the reality. I'm a lawyer. That's the law.

Now, let's talk about the world we want to create. If we want to talk about the world that we want to create, I think it requires a combination of national laws

and international agreements. And the best way to discourage protectionist forces is actually to have some international norms so that governments know when they have access to data in another country and under what terms and it's subject to a consensus that people, the publics in these countries, are comfortable with. And the more you build the Internet, these international norms, the better able one will be when it comes to addressing protectionist pressure or other things that would place more national restrictions in place.

MR. KERRY: Other questions? Yes, sir, in the blue shirt back there? The microphone is coming.

QUESTIONNER: John Hanchak. I'm with Georgetown among other things. I'm from the West Coast, so this idea --

MR. SMITH: So am I, by the way.

QUESTIONNER: Yeah. The cyber sphere and all of that, we can argue whether or not it's coming. But there seems to be an issue that we need to address here directly, which is privacy. What does it mean? There's been a decoupling like you said of secrecy from privacy, and yet there's a terrible imbalance. Individuals have no secrets, but the government and companies have many secrets. We have no way of rebalancing that. It seems a losing battle to try and protect privacy as we've known it. It's not working. We are skirting around all of these issues of hiding the data and moving around. It's not like a safety deposit box. It's accessible.

So it seems almost that we need to move towards something different, something radically transparent. If everyone's watching everyone, then we have something where everyone's accountable. This is a frightening world. We've never quite had this. Maybe in the village days we had this, but we've never quite had this before in this way on a global scale.

But this is something that I think a lot of people have been talking about. How do we rebalance secrets? The FISA court may be working well like you had said,

but we don't know anything about it. We're not involved at all. So people become afraid, and they don't trust when they don't know. We're all in glass houses, but somewhere above us is a giant steel box with telescopes. This is not sustainable. We won't trust. We don't trust the companies because the companies still have secrets.

So it seems we need to start getting individuals more involved because there are people around the Earth looking at how to do this. You know the West Coasters. They're going to build these tools. The nefarious people already have these tools and they use them. They use Tor and they use Bitcoin even though Bitcoin is flawed. But these technologies exist and you can use them. So I guess the question becomes: how do we make sure that government is still involved in a world where many people want to leave it behind?

MR. SMITH: Well, the only thing I would say -- and I know we're almost out of time, so we have time perhaps for one more question -- but one thing I would say is look, in many ways it's new and in many ways it's not. Communications technology has been advancing literally for two centuries. And I think the fundamental question we all have to ask ourselves and the fundamental question I think you're raising, is what enduring values do we want to continue to enhance? Technology can threaten certain values. It can advance other values. But ultimately it is the role of a free society and its government to decide what enduring values it wants to invest in. And I think that is something that is more necessary because of technology even if technology might threaten it, and I think getting more people involved as you point out is part of the answer.

MR. KERRY: So we have time for one more question. Please make it short. Ma'am?

QUESTIONER: Thank you. My name's Natalie Marshall. I'm a doctoral student at the University of Southern California. My question is about private sector companies both in the tech sphere and telecommunication industries and other Internet providers that, unlike what you're describing about Microsoft and the rest of the U.S. tech

sector, don't see themselves as having a role to play in the protection of these citizen-consumer people who have privacy and civil and human rights.

How can the advocacy and nonprofit sector help these companies who don't see things the way that you do to understand their role and be more responsive to consumer demands and expectations?

MR. SMITH: A great question and it's certainly I think a good question on which to end and I would say two things. First, it's why there is a vibrant discussion today and why there needs to be an even more vibrant discussion in the future that brings together people from government, people from academia and the NGO community and civil society, and people from the industries and companies that are creating and deploying these technologies. I don't think one can have a true lasting approach without bringing all of these groups to the table and having this kind of conversation. So I just think it's a prerequisite.

And I do just think finally it's sort of takes us back to where we began. We are having a national debate as a country. I think interestingly there are aspects of this debate that are getting more attention outside the country than inside the country. Certainly you can't spend time in Berlin or Beijing sometimes without coming to that conclusion. And I think it's important for us in the United States to have a broad perspective on how the world is thinking about this.

I think we need to continue down the path we've started, and we need to finish what we started when it comes to rules for government surveillance. I don't think we've gone far enough and we need to do more.

And then finally we need to recognize that we do need, in my opinion, a broad-based legal and regulatory model when it comes to company use of personal information. I'll just say this. Imagine a bank that doesn't take good care of its customers' money. Do you think it has a bright future? What do you think of a tech company that doesn't take good care of its customers' information? I believe that over

the long term, the world will expect and even insist that we pay as much attention to the personal information of consumers as banks do to their money. And the sooner we get started on that and the faster we come together to have the kind of broad-based conversation that you're referring to, the more successful we're likely to be.

MR. KERRY: Well, Brad, thank you. We are in the midst of what President Obama called a national conversation about privacy. You've been an important part of that conversation with the President in public and here today. It's an important conversation. It's, I think, a critical issue to enable some of the benefits that you've talked about. It's a conversation that clearly has a lot of layers to it, and I thought we had some very thoughtful questions here today.

So we want to thank you for being here. I want to thank all of you for joining us and for your questions. This is a conversation that clearly could go on today, but it'll have to continue in other forums, I'm sure, for a long time to come.

Thank you very much.

MR. SMITH: Thank you.

* * * * *

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.

Carleton J. Anderson, III

)Signature and Seal on File)

Notary Public in and for the Commonwealth of Virginia

Commission No. 351998

Expires: November 30, 2016