RSA Conference

Company Participants

- Bradford L. Smith, President & Chief Legal Officer
- Unverified Participant

MANAGEMENT DISCUSSION SECTION

Unverified Participant

Ladies and gentlemen, please welcome President and Chief Legal Officer, Microsoft, Brad Smith.

Bradford L. Smith {BIO 1721351 <GO>}

Good morning. I want to begin by saying that it's a pleasure and a privilege for me not only to represent Microsoft here at this 25th conference, but in particular to follow Art Coviello on to the stage. Art, I think the most important thing to say is you have not only accomplished great things in your lifetime, but as someone who just received a lifetime achievement award, your life hasn't over yet. There are new things I'm sure. And we at Microsoft will look forward to following them.

I'm here today because I want to have a conversation. A conversation about the issues of the day and share a little bit about what we are thinking and doing. And more importantly what we all have the opportunity I believe to think about and act upon together.

I think it's worth reflecting on the fact that the debates of the day may seem new, but in many ways they're just a new chapter. A new chapter in a discussion that is as old as this country itself. Because since the earliest days of this country, technology has been an engine of change. It has been an engine that has enabled people to do new things. But in the process it has raised new issues, and it has unleashed new debates.

At times technology has literally been an engine of change. Did you know that before the transcontinental railroad was completed in the late 1860s, it took over three months to travel from New York to here in San Francisco. But even more than that, 30% of the people who started the trip in New York would die before they got here. Once that railroad was finished, it took a week. And almost everybody who stepped on the train in New York knew with certainty that they would step off the train here in San Francisco. But technology, the railroad, changed every aspect of society. It changed every field of law. It unleashed public debates that actually took several decades to resolve.

And when Henry Ford invented the Model T 105 years ago, we saw the same thing ensue, decades of important debate with the public about the role of regulation and the role of innovation and safety for technology.

Meeting here today, we are the latest generation. And we're here to talk and think about the latest generation of technology. As we think about the issues of our time, we need to reflect, I believe ,on the events of our time. It is a tumultuous and even turbulent time in which we live. And we see this in the days that shape our years and our lives. And there are certain days that stand out and shape the way all of us, I think, have the opportunity to think about these topics.

Certainly one important day in recent years was December 19, 2013. It was a day when the news came out of Minneapolis, and Target informed the world that over 40 million customers had suffered a hack, as their machines in stores had been penetrated. Within less than a month, Target was obliged to say that the number of people who were affected had topped 100 million. And the investigation that ensued literally took people around the world. That was one episode that opened the world's eyes to the importance of these security issues for technology

But there was a day that I think opened people's eyes even more. It was in the following year, on November 24, 2014, on a Monday morning in Los Angeles. Millions of people got up, and they drove to work the same way they do every Monday morning in LA. Some of them drove to work by driving through these gates, little imagining that, as employees of Sony Pictures Entertainment, they were about to become part of what Fortune magazine would call the hack of the century.

And as their computers failed to operate as they expected, as investigators got to work, little did people expect that their work, as in the Target case, would take them halfway around the world to North Korea. And little did they imagine that they would become embroiled not only in an issue of IT security, but an issue of geopolitics. As in Washington DC on December 19, 2014 – coincidentally one year to the day after Target had made its announcement – President Obama gave his annual press conference. And the last thing he talked about before boarding Air Force One to start his annual vacation in Hawaii, was to say this.

[Video presentation] (5:23 – 5:46)

This, as much as anything else, perhaps more than anything else, shows how much the world has changed for our customers as an industry. IT administrators now find that their work can be the subject of a critique at a presidential press conference.

But the world has changed in other ways as well. And we're sensitive to that. I believe we all are. We need to reflect on that aspect too. We see it in the other days of our lives. We saw it last November, on the 13th in Paris. When on a Friday evening, people started the way they start every weekend in Paris, by going out. But at 9:30 that evening, a man walked into a café on the Boulevard Voltaire, he sat down at the counter. He calmly ordered a meal. And nine minutes later, he blew himself up.

Within moments, the streets of Paris were filled with the sounds of sirens and the sights of police cars. And the next morning, the sights at the Boulevard Voltaire and other streets were filled with flowers mourning the victims of the previous evening.

And of course it was just a couple of weeks later, when on another part of the world in San Bernardino, California, the images were all too similar. Police cars in the street and that night candles held by mourners for the 14 victims who had been killed.

Immediately those issues connected with our issues, as people went to work debating whether this meant new steps needed to be taken for technology, for surveillance, for encryption. We live in a world where every week there is a pendulum. And the question is, which way will the pendulum swing on these issues that affect us?

I think it's worth recalling that all of these questions reflect among other things the role of technology and the way it has changed. The Internet started out two decades ago as something people talked about as a different space, Cyberspace, as if it was disconnected from real space and the real world. But what we have learned today is that if people want to shape it or impact what happens in the real world, they go to the Internet, whether it's to recruit people or to espouse their views or to investigate crimes, to learn, to study, you name it. The real world now often starts with what happens on the Internet.

And this has affected everybody. Governments around the world studied the Sony case. And they realized that there is no such thing as national security in this decade without cyber security. We've studied it as an industry and as security professionals. And we've recognized that we cannot keep people safe in the real world if we cannot keep people safe on the Internet.

And this is true not only for enterprises but for consumers, for young people, and for the elderly, and for everyone in between. We've realized that hence we need to keep information secure. We need to keep information secure. Because in no small measure has a unanimous Supreme Court recognized two years ago, the contents of a smartphone or any computing device today contain the privacies of life.

More so than ever before, one thing is clear above all else. People will not use technology they do not trust. And as trust in the absolute foundation for our entire industry. And it needs to remain that way.

But as all of this has been unfolding, another thing is clear as well. Trust has been under threat. Trust has been questioned for good reason since this individual, a person we all now recognize, Edward Snowden, got on an airplane, took four laptops with him, and began to tell the world things that the world was not aware of before.

And all of this is leading to a fundamental question, what's to be done? That's the fundamental question for those of us in this room. It will be the fundamental question later today at a hearing in Congress. It is the fundamental question for this country. And it's the fundamental question for the world.

I think whenever you have a question that is this important, it's always worth starting by reflecting on the fact that no one person has all the answers. We need to have a conversation among ourselves and with the world.

We at Microsoft don't have all the answers. But we've certainly spent a lot of time thinking about this. One conclusion that we've come to is a point that Satya Nadella, our CEO, made to our employees two years ago. What he fundamentally said is technology needs to advance, but timeless values should endure. And we always need to reflect on what those timeless values are.

As a company we spent time and we formulated four principles to guide our decisions. That security is paramount. We need to keep people's data secure. We need to recognize that when people entrust their data with us, they still own their data. We do not. We need to protect their privacy. We need to manage people's data in accordance with the law. And perhaps most important, we need to be transparent, so people know what we're doing.

But it's not enough to be able to articulate principles on paper. We need to put them into practice, as companies and as an industry. And that's what we've been trying to do. It's what we're focusing on doing every day.

For two decades our industry, security professionals has talked – have talked about protecting, detecting, and responding to security threats. I think that foundation remains as important today as it was the day it was first defined. But we need to evolve it forward.

We each have an opportunity to step up. We each need to step up. Certainly as a company, we're focused on taking a holistic approach. Satya announced in Washington DC last November that we're now investing $1 billion a year as a company in new security technologies and practices. We've recognized that we need a holistic approach, an approach that starts with identity, but then considers devices and applications and infrastructure and data itself. And as we think about all this, we need every day I believe to keep in mind that when it comes to security, there is no technology that is more important than encryption.

That's why we need to stand up, be thoughtful, and also be vocal. Despite the best of intentions, one thing is clear, the path to hell starts at the back door. And we need to make sure that encryption technology remains strong.

But we – there may be no part of the debate that is more important than the debate about encryption. But it is not the only part of the issue or the work or the debate that matters. And we need to remind people of that as well.

Certainly as a company, we're striving to take a holistic approach, an approach that focuses on strengthening our platforms, Windows and Azure and Office 365, an approach that recognizes perhaps as many – as much as anything else – intelligence. Big data is a game changer here.

As a company, we have trillions of data points coming in from billions of endpoints. And it's that ability to understand and gain insight and take action from that data that can make all the difference. And we need to partner, because no company is going to be successful on its own.

At a time when technology is moving forward and is so vital, we need to remember that this is, at the end of the day, all about people. That's why we at Microsoft have created a Cyber Defense Operations Center that brings together all of our security experts across the company, so they can work in the same place elbow to elbow. We love Skype. But we actually like people to talk to each other in person as well.

We're focused on moving forward across the board. Last week we announced the new steps we had taken to secure Cloud apps and SaaS applications. We announced new steps that we had taken to add new security features for Office 365. And this morning, we announced new features at a new Windows Defender Advanced Threat Protection to better secure the client for enterprises as well. Something we describe for people, as you'll see here.

[Video presentation] (15:10 – 16:56)

That's a reflection of the type of step we're trying to take as a company. I think there's lots of companies that are here that are taking vital steps forward.

But as important as the steps that we're taking as individual companies are the steps that we have the opportunity to take together. As we take these steps together, I think it's worth reflecting on what I believe was one of the most important things that Steve Jobs ever said. He said that every day, he aimed to be at the intersection of engineering and the liberal arts. Almost five years after he passed away, that intersection is more important than it has ever been before. Regardless of what you might have majored in in college, regardless of the field that you claim to be your own, I would argue that we all need to work at this intersection. It is a complex world. And we need to work together.

That's why, in some ways, it's interesting and even unusual that I stand before you not only as somebody who has worked at a company like Microsoft with engineers every day for over 22 years, but as somebody who is a lawyer and has a law degree. Because as much as ever, these issues are being defined not only by our investments and steps in technology and engineering, but by the commitments we need to back, by our legal resources as a company and an industry as well.

In this area, as in others, we need to step up and we need to stand for things. But I also think we need to be broadminded. We need to constantly remind the world of all of the things that we are thinking about. Clearly as an industry we not only have a role, we have a responsibility, I believe, to help keep the public safe. That's one of the points that Apple is making in Congress today.

It's why we at Microsoft for years have had a Digital Crimes Unit. It's why we've been so privileged to partner with other companies in our industry to act against security threats like botnets. It's why we're taking new steps to protect the most vulnerable people, whether they be our youngest or the oldest members of our society. It's why when things go wrong, people often call tech companies. Microsoft like Apple has people that literally are on duty 24-by-7.

One thing we haven't shared previously with the public is this. In the days and weeks after the Paris attacks, Microsoft received 14 lawful orders seeking content about terrorist suspects that were at that point at large in France and Belgium. In all 14 of those cases we were able to respond, determine that the orders were lawful, pull the content, and turn it over. And we did that in an average response time of under 30 minutes.

We do play our role as an industry. But we also need to stand up for customers. And that's what we've tried to do in other cases. We believe emphatically that when the government wants to investigate a legitimate business, that it wants information that belongs to that business, it should go to the business and serve a warrant or subpoena on the business and not go to the cloud services provider instead.

This is the way that law enforcement and the law have worked in over – in our country for over two centuries. Cloud computing should not change that balance. Businesses have a right to know so they can defend themselves. And it's why we at Microsoft are joining other companies across our industry to stand up for and stand with Apple in this new important case.

As we think about what it will take, both to keep the public safe and to stand up for our customers, there is a principle that cuts through everything. And it's called transparency. If people know more about what is happening to their data, whether it's the actions of companies or steps by the government, they will be empowered to make more informed decisions as consumers and as citizens and as voters.

That's why we at Microsoft took the unusual step of filing a lawsuit in 2013 against our own government. We went forward, as did Google, and we asserted that we had a constitutional right under the First Amendment to share more information with the public.

Now this was an unusual lawsuit. It was before what's called the Foreign Intelligence Surveillance Court. Most courts of the United States have a courthouse, they have an address, they have a phone number. You call, someone answers. This court is different. When you call the phone number, this is what you hear.

[Audio Presentation] (22:18 – 22:24)

Litigating before this court was different from anything we'd ever experienced. Typically, you file your brief, you hand it in, you wait for the brief to come back from the other side, then you can read what they're arguing against you. When we received the brief back from the government, we opened it up, and it was little hard to tell what the government was arguing.

We didn't stop at the courthouse. We took our case to the White House. We took our argument to President Obama. And on January 17, 2014, he went to the Justice Department. He gave a speech, it started to put this country on a path to surveillance reform. And the government agreed to settle the lawsuit so that we could share more information. And that has been important.

Companies across our industry have taken important steps. And I think we should give credit to where credit is due. So here I am on behalf of Microsoft to show you the folks at Google did a great job. We all had the opportunity to learn from them the way we all have the opportunity to learn together. Certainly we at Microsoft, as we've created our own transparency hub, have tried to continue to move forward the edge of the envelope and share more information.

We also need to keep in mind that we have a responsibility, not just to the people of one country, but to the people of every country. In the world today, only 4.5% of the global population lives in the United States. We have to keep in mind the needs of the 95.5% of the people who do not.

That's why we as a company took the step of raising another lawsuit, a lawsuit that started when the U.S. government sought to take a unilateral search warrant to pull email out of our data center in Ireland. And we've gone forward, and we're continuing to argue as this case goes up the appellate ladder, the governments actually need to respect each other's borders and respect each other's laws. People have rights to privacy. And they deserve the right to have them governed by their own law.

And as this case has moved forward, we've received broad support, not only from across the industry, but from across civil society. There have been amicus briefs filed by 28 technology and media associations, 23 advocacy and other groups, 35 of the leading computer scientists in the United States, and even the government of Ireland itself. The day these briefs were filed at the end of 2014 is the only day that I can recall when Fox News and the ACLU were actually on the same side. That's how broad the support for this point of view is.

Ultimately, I think we also need to reflect upon the fact that we need a world where technology is governed by the rule of law and not simply the laws of physics. We need good law. But this is not about creating a world where technology is above the law. Just as it is not about creating a world where any government or any person is above the law.

It's important for us always to keep in mind that this is an issue that poses timeless values that we need to move forward together. Public safety and personal privacy and freedom of expression are all values and principles that matter. And there will be some days when a balance will need to be struck. And that balance should be struck not by those of us who are unelected, but by those people who are. That's why especially in democratic countries we need governments to strike the balance.

But it needs to be a well-informed balance. This is why we believe that a new piece of legislation that was introduced in Congress yesterday by Senator [Mark] Warner and Representative [Michael] McCaul would do the right thing, bring together a commission of experts to advise Congress on encryption. Because that is the only way to ensure that our elective representatives are well-informed in the best possible way. And it gives us the best possible opportunity to move the law forward. That is also a big part of what we need to do.

We live in a world where some things improve with age, but other things do not. Law and especially technology law does not improve with age.

I pointed out last Thursday when I testified before the House Judiciary Committee, the same committee that is having a hearing today, that the principle law in this place in the United States, the Electronic Communications Privacy Act, was passed in 1986. And the day the House passed by voice vote that piece of legislation on June 23, 1986, Ronald Reagan was President, Tip O'Neill was Speaker, and Mark Zuckerberg was two years old.

A lot has changed. The computers that we use today were barely within the grasp of our imagination. When I showed that committee our latest computer, the Microsoft Surface, I pointed out that not only is it connected to all the world's information on the Internet, but by itself this smaller device stores 355,000 times as much data as the floppy disk that one had to use in 1986. But even that does not actually capture the full gap between technology and the laws that our courts are trying to grapple with.

We've all had an opportunity in recent weeks to read about this law that frankly most lawyers seldom talked about, the All Writs Act. It goes back to the founding of the country. It was last amended I think in any significant way in 1911. And as I showed that committee last week, the most advanced computing device of that era was sold in 1912, a year later. It was an adding machine. It was this adding machine.

We do not need our courts to define the legal rules that will govern 21st technology technology – 21st century technology with laws that come from the era of the adding machine. We can do better than that.

So in conclusion I would say this. We need to be thoughtful. We need to be broadminded. But as much as anything else, we need to use our voice and we need to act. We should come together as a community. We should heed those values that truly are timeless. We should support fundamental rights. We should keep technology secure. We should continue to help keep people safe.

We should always keep in mind technology has moved forward. Technology needs to keep moving forward. It is our job to advance and innovate in technology. But we can't do it in society in a vacuum. We need to connect with the world. We need to connect with people across this country. We need to engage in public debate, because the world is going to trust technology only if the law can catch up. Thank you very much.

This transcript may not be 100 percent accurate and may contain misspellings and other inaccuracies. This transcript is provided "as is", without express or implied warranties of any kind. Bloomberg retains all rights to this transcript and provides it solely for your personal, non-commercial use. Bloomberg, its suppliers and third-party agents shall have no liability for errors in this transcript or for lost profits, losses, or direct, indirect, incidental, consequential, special or punitive damages in connection with the furnishing, performance or use of such transcript. Neither the information nor any opinion expressed in this transcript constitutes a solicitation of the purchase or sale of securities or commodities. Any opinion expressed in the transcript does not necessarily reflect the views of Bloomberg LP.