

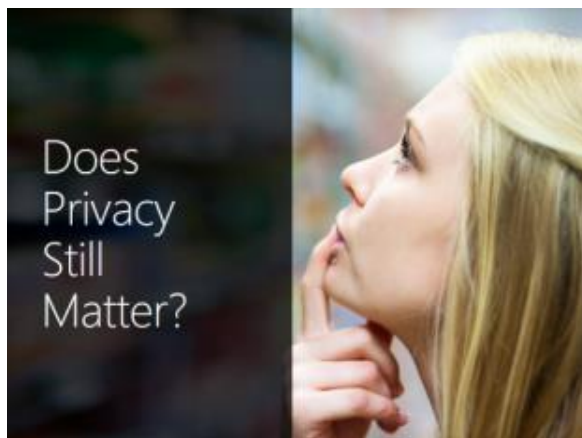
**Putting People First:  
Moving Technology and Privacy Forward**

**Brad Smith  
General Counsel and Executive Vice President,  
Microsoft Corporation**

**Transcript of Keynote Address at the 34th International Conference  
of Data Protection and Privacy Commissioners  
Punta Del Este, Uruguay  
October 23, 2012**



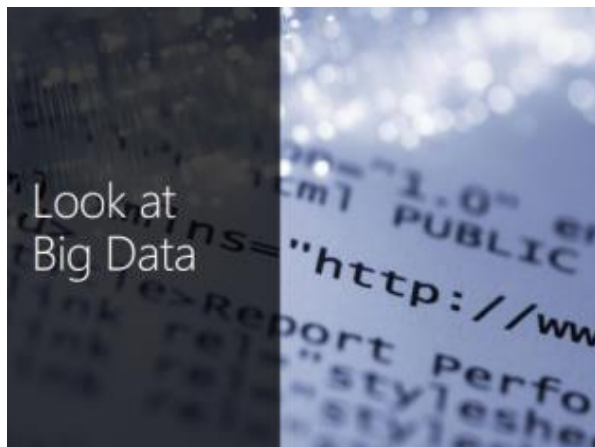
Thank you so much for the opportunity to be here this morning. I've made many trips to Latin America before, but I suspect like most of you I've never had the opportunity to experience a cyclone firsthand. (Laughter.) I suspect that a year from now you may not remember a word that I utter this morning, but I guarantee you that every one of us in this room will remember the weather when we got up; it's been that kind of day.



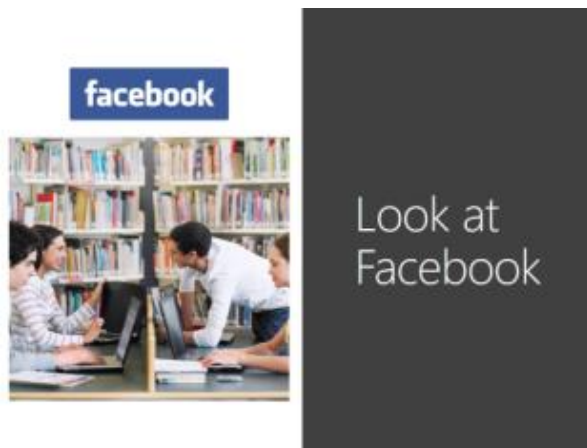
We come together to talk about an important topic, privacy, but despite the evident importance to all of us I think it makes sense to start by asking a question: Does privacy still matter?

It seems obvious to us that it matters. After all, we came all the way to Uruguay to have this conversation about privacy. Clearly it must matter.

But as you may know, I work in an industry where one frequently encounters people who actually want to debate whether it matters. They want to talk about how it matters, they want to talk about why it matters, and they want to talk about whether the way it matters has, in fact, changed over time.



They point out, for example, that if you look at big data, privacy must not matter as much as it used to. After all, look at all the information that people are sharing. Look at all of the good ways in which it is being used.



Or sometimes I meet people who say, look, privacy must not matter, at least not the way it used to; after all, look at Facebook. There are a billion people in the world who are sharing all kinds of personal information about themselves. How can Facebook be such a success if privacy still matters?

Well, the first thing I have to say is this: let's look at Facebook, and let's look at the Facebook story. I'm not here to be an

expert on Facebook's privacy policies, but I can speak as somebody who was involved in the decision at Microsoft *exactly five years ago today* to invest \$240 million in Facebook.

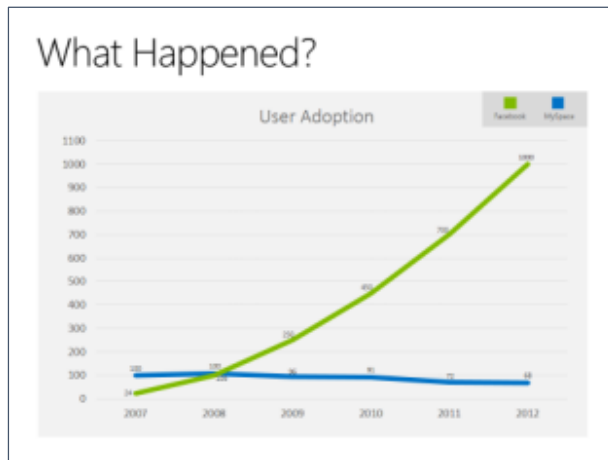
Now, at the time, it was not necessarily obvious that Facebook would ever have a billion users. At the time, Facebook was not even the most popular social network on the



planet. It wasn't the first. The first was probably a service called Friendster.

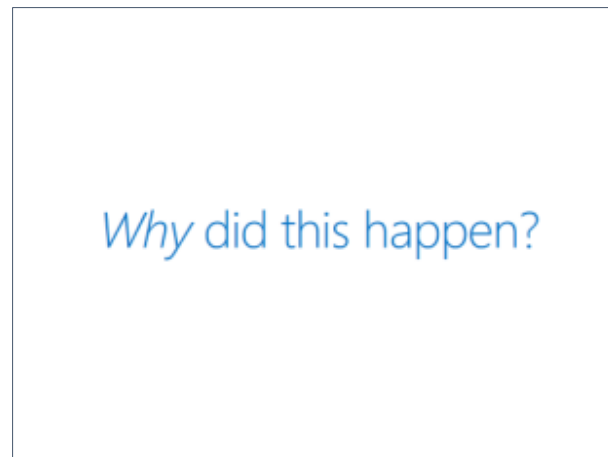
It wasn't the second. The second was a social network that became very popular called MySpace. In fact, five years ago, MySpace had 100 million users, Facebook had only 24 million. In our industry it is very unusual for one company to be the first to reach 100 million users and to have four

times the market share of its next closest competitor and not go on to be the prevalent and most popular service by far.

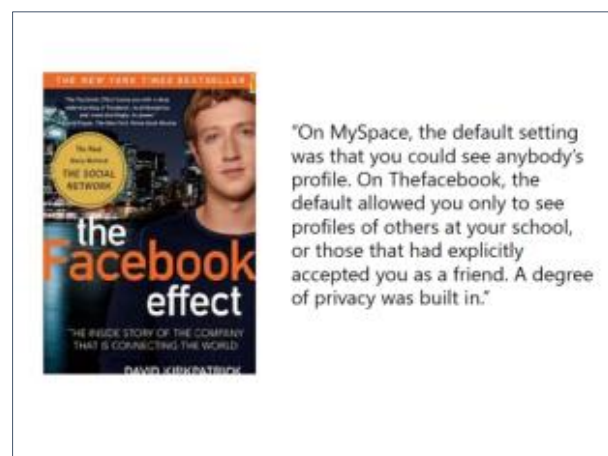


But, of course, the real question here is, what happened? What happened over the last five years?

Well, at a certain level I think we all know what happened. MySpace didn't do so well. It has fewer users today than it had five years ago. Facebook has exploded. In five years it has gone from 24 million users to a billion. We've done pretty well with our \$240 million investment.



But I think the most important question for us is not what happened, but why. Why did these two curves take off the way they did in such different trajectories? There are a number of different reasons, but there is one that personally I think probably matters the most. It's certainly one that we thought about when we put \$240 million into the company.



It's a facet that was captured well by one of the leading books about what happened, David Kirkpatrick's book when he addressed why this happened.

And what he said was on MySpace, for people who remember it from five years ago, the default setting was that you could see anybody's profile. Or to put it another way, the default setting was anybody could see your profile as well. But on TheFacebook, and initially it was called

TheFacebook, the default allowed you only to see profiles of others at your school or those that had explicitly accepted you as a friend. A degree of privacy was built in at Facebook by default in a way that was simply not the case at MySpace.

## A Key Difference in Approach

Sharing by Default



myspace®  
a place for friends

Sharing by Choice



facebook

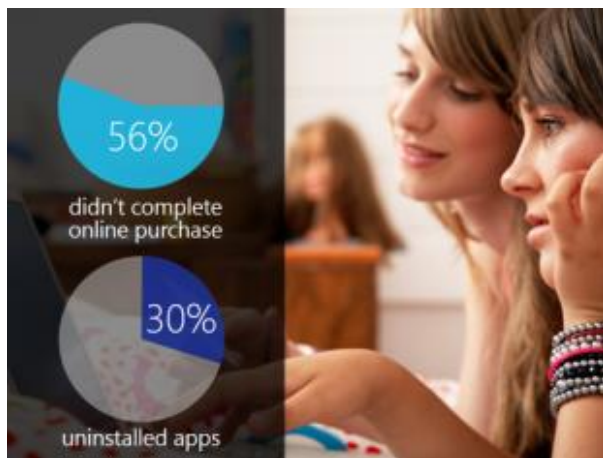
So, in effect at MySpace you could change the settings, but by default you shared your information with the world. And at Facebook by default you shared information only with people in your network and the people that you decided to make your friend.

It's not just the votes of consumers in their adoption of Facebook that tells us, in my opinion, that privacy matters to people – that privacy matters to consumers.

Consider this: Recently the Pew Research firm did some research in the United States, and what they found was that 56 percent of consumers had decided not to complete an online purchase because of concerns about sharing personal information with the seller that they were going to do business with.

They also found that 30 percent of consumers had uninstalled an app from their smart phone because of concerns about the way that app dealt with their personal information.

If you put these things together, I think they tell an important story. They tell us that people care about privacy.



People care about privacy.



People are thinking about privacy in new ways.

But that's not the whole story, because I think they also tell us that people are thinking about privacy in new ways. And if we're going to do our jobs well, whether we come to this meeting from industry or from an NGO or most importantly from a government and as a regulator, we need to really think about the new ways that people are thinking about privacy.

Technology and Societal Change



To start with, I would say in many ways this is not a new phenomenon. The history of technology is a history of societal change. Typically one sees a pattern. The pattern starts with the invention and then the increasing adoption of new technology. That is then followed by a second step in the process. That second step involves new consumer needs and new consumer views about what to do with respect to the technology. And then finally, there's a third

step. The third step is about what all of this means for laws and for regulation and for public policy.

"The Right to Privacy"  
Harvard Law Review, 1890

"Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual ...the right to be let alone."



And indeed the story is well documented. The truth is, as many of you are aware I appreciate, the whole global discussion about privacy really began with this invention on the screen, the camera in the 1800s. And interestingly, as the camera became more popular, as it was found throughout society, we saw this pattern take place. By 1890 there was a famous law review article in the Harvard Law Review written by Professor Louis Brandeis, who would go on eventually to become a justice

on the U.S. Supreme Court. And it was in this article that Professor Brandeis coined the famous phrase, "the right to be let alone," a phrase that many people who work in the

privacy field every day are familiar with. But interestingly that phrase is at the end of a sentence that starts by talking about technology.

What Professor Brandeis recognized was that the camera had changed society. And because the camera had changed society, people could no longer walk out of their front door without the risk of being photographed. And, of course, this was before there were lenses that could see someone a kilometer away. And he recognized that because of this invention there was a new legal right that needed to emerge to protect people the way they had always been protected in the past before this technology had entered the scene.



And we see 122 years later the leaders of our day in the United States and around the world grappling with similar phenomena. It was in the State of the Union address this year and in other reports at the start of the year that President Obama started to address these issues. I think he captured part of this issue for us very clearly, because what he said is that we live in an era where people are sharing more information, but that does not mean that privacy is an

outmoded value.

What we really need to focus on, in my opinion, is how to reconcile these two aspects. And indeed we meet in the year 2012 when people around the world are doing just that.



Personally, I think that perhaps the single most important statement in the United States this year came in a case from one of our current Supreme Court justices, Sonia Sotomayor. The case involved Jones versus the United States and the question of whether the police needed a warrant to put a GPS tracker on a car.

As many of you may know, there is a constitutional right to privacy under the

Fourth Amendment to the U.S. Constitution, and that protection always turns on whether people have a reasonable expectation of privacy in a particular situation.

But Sonia Sotomayor, Justice Sotomayor, had something very interesting to say. She said that for over a century people in the United States had always looked at the Constitution and, in fact, said that there was a reasonable expectation of privacy only if there was a reasonable expectation that people could keep certain information secret. And, in fact, I think, if you read much of what had been written about privacy over the last 50 years, in many, many instances, perhaps most, if you substitute the word secrecy for the word privacy, the meaning of a sentence or the meaning of a paragraph is unchanged. When people were talking about whether they could keep something private, they were, in fact, talking about whether they could keep something secret. Certainly in the United States that has been at the core of our legal evolution.

But I think the question that Justice Sotomayor posed, while focused on the Constitution, was, in fact, far broader than that: Is secrecy still a prerequisite for privacy?

Consumers want to  
*share* more personal  
information.

I think that if you look at the world today, if you look at the story of Facebook, if you look at the story of people using the Internet, one thing first is clear: People are less focused on secrecy. Consumers want to share more personal information than ever before. They don't care as much about keeping things secret.

*BUT...*

But that doesn't mean that they don't care about keeping things private, because there's a big "but" involved.

They want to decide  
*who* they share  
information with.

The fact is people want to decide who they share information with. People of all generations want to make that decision themselves.

AND...

And not only that, they also want to determine how their information will be used by the people with whom they share it.

They want to determine  
*how* this information  
will be used.

That's the new model for privacy, not a model focused on secrecy but a model focused on what people are saying: they, in fact, want and need the ability to decide who they share information with and how that information will be used.





And when you step back and think about this, I believe these are reasonable needs. These are laudable goals. And from every vantage point, our preeminent obligation should be to help people meet these needs in a world of new technology.



Now, life would be simple if that were the only goal we had to meet, but as we know, it's not very simple at all. The reality is we need a balanced approach to address privacy. We need a balanced approach because more is at stake than solely the protection of privacy, as important as that goal and need, in fact, is. There are other goals that need to be addressed and balanced with it.



For one, it is important to ensure that innovation flourishes. It's important to ensure that innovation flourishes because innovation does so much in the technology space to help people around the world.

Certainly in the technology sector this is something that we see every day. It's why many of us have chosen to spend our careers in technology.



We see it today in the benefits of big data. We see it in ways that are profound. We see it in stories that people in the technology field bring to life every day.

One recent example, in fact, involves the use of search terms in Bing. It turns out that when the Food and Drug Administration in the United States, like most authorities around the world, approves a drug, it focuses on that one drug alone. But it also turns out

that millions of people every day in every country in fact use more than one prescription drug during the course of 24 hours. No drug authority can possibly test the combination of every drug with every other.

But last year, a researcher at Stanford started looking at the potential side effects of what might happen if people took two drugs together. One was a drug that is an antidepressant. It is an antidepressant that is taken by millions of people in North America and tens of millions of people around the world. The second was a drug that reduces cholesterol levels. In fact, these are two of the most common drugs that doctors prescribe.

But this researcher began to become concerned about the possible side effects of what might happen if people took both of these drugs together, side effects that no one had diagnosed. He began to review certain data that was in the possession of the Food and Drug Administration in the United States, and then asked us at Microsoft if we could share with them in a de-identified manner certain search terms that had been entered in Bing. And specifically what they wanted to search for is search terms where people were entering in the name of one or both of these drugs and some of the symptoms associated with diabetes, such as fatigue or headaches.

And what they found is that when people searched for only one of these two drugs it was unusual for them to include in their search request one of those words, but when they entered a search request that had both drugs together, a full 25 percent of the time they were also looking for information about how to deal with a headache or how to address fatigue or other symptoms associated with diabetes. And this helped the Stanford researchers along the path to a conclusion that if you take these two drugs together, you do face a potential side effect of having diabetes.

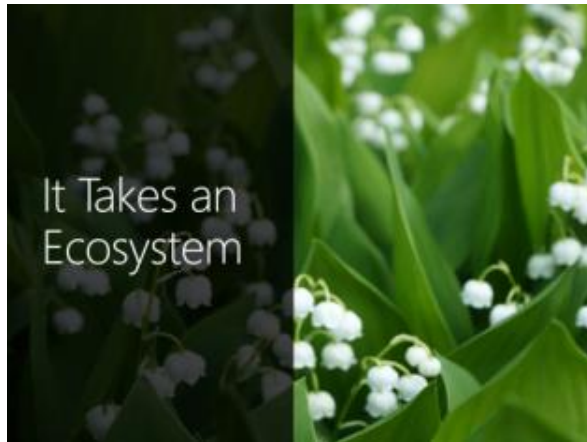
There are a million Americans in our country alone that happen to take both of these drugs, and for them, this kind of insight, when shared with doctors and applied with their patients, is something that can save a life. In fact, it's something that can save many lives, and it is made possible in part because of the insights that come from our use of big data and information.



It's not just innovation and big data, though, that's at stake. There are other things as well.

We find every day that the use of information is of fundamental importance in our ability to make technology stronger. As we think about the various products and services that our customers use, many of them, for example, use more than one e-mail service, or they may use differing e-mail services because we offer more than one. And if we can take what we're learning from users and then apply it in a properly de-identified form, it enables us to strengthen protection against malware and against spam, not just in the first service where we might have seen a problem arise, but across our products and services. And in so doing we make technology better able to protect our customers.





And finally, we appreciate that, in fact, the success of the Internet and all the benefits it provides are based not on a single technology. They're not based on a single company. It takes an ecosystem to succeed.

And we need to be sensitive to all of the groups in the ecosystem, including advertisers, because we appreciate that it is precisely because of advertising that there is so much free and low cost content available to consumers around the world on the Internet today.



So, ultimately we need to think about privacy and innovation and the protection of consumers and the value of advertising.



If we're going to do all of that, we're going to need some fresh approaches.

As we've certainly thought about it, a few things have become important in our minds. First, we need to recognize that some of the things that we have been relying on to protect privacy are not doing the same thing they did before.

If I think about so many of the discussions that I have been involved in on this issue since the early 1990s when I lived and worked in Europe, it's clear that a fundamental tenet, perhaps the core tenet of the protection of people's privacy, has been the concept of notice and consent.



We've done a lot of work across our industry to improve notice and consent, and people in our industry take pride that we can share a lot of information, and it may only take you 10 minutes to read it.

The problem, as two researchers at Carnegie Mellon recently found out, is that with the ubiquity of Internet content and technology products and services, people are given a lot of privacy notices to read. In fact, as

they found, over the course of a year an average consumer is asked 1,462 times to read a privacy notice. Well, if you take 10 minutes and multiply it by 1,462, what you find is that people would have to devote 76 days out of their year to reading privacy notices in order to understand what, in fact, they're encountering when they use these services. I don't think any one of us in this room would ever expect consumers to spend seven days a year, much less 76 days a year, reading privacy notices.



What that tells us, I believe, is that we need some new approaches as well. We believe that part of the answer comes in Fair Information Practices – best practices that have received the support of a broadening consensus based on several decades of discussion, practices that have been embraced and endorsed in international fora around the world, practices that go to the heart of so many of the issues that are so important to privacy: transparency,

accountability, limitations on use, as well as notice and consent and others.

More and more, we will benefit if we look to Fair Information Practices to help complement and even in some situations perhaps even replace specific scenarios around notice and consent. We need to think about this an increasingly important tool in our toolkit.



We need a combination  
of approaches.

But we also need a combination of approaches, and I think at bottom we really need to think about three things and how they come together.



First, even though I represent a technology company, I believe in the importance of privacy regulation. I believe we need clear and fair rules of the road. We need rules of the road that increasingly apply consistently in country after country and continent after continent. We need clarity so that everybody knows what they need to do, and companies that act responsibly are not going to find themselves suffer at the hands

of companies who do not, and regulation creates that floor that provides that level playing field.

But we don't need regulation alone. We also need self-regulation. We need self-regulation especially in the form of industry standards. We need self-regulation that can move technology forward, and we need self-regulation that can move faster and more globally than regulation alone is able to do.

But even these two things together, in my opinion, are not sufficient. At a time when everyone is talking about standards, it is important, I believe, to remember that we need market-based innovation as well. With market-based innovation there is an opportunity for companies to experiment, to try new things, to see what consumers want, and if consumers do, in fact, want what companies are offering, there's an opportunity for those companies to grow. Market-based innovation is every bit as important, in my opinion, as these two other ingredients as well.

We need to come together.

All of this makes for a sometimes complicated conversation, and certainly in my role at Microsoft one of the things that I've come to conclude is that we need to come together. We need to come together to work through the complicated conversations we need to have.

DNT.

And there's probably no topic that I've been involved in that has involved more complicated conversations over the last couple of years than three little letters that I've come to know by heart: DNT. And so I'd like to conclude by offering a few thoughts on DNT, or Do Not Track.

As a company we have taken a stand, if you will, when we decided earlier this year to turn on the Do Not Track signal in the new version of our browser and the new version of our operating system that starts to ship this Friday.

We've had to think a lot about DNT. Whenever you have to think a lot about a topic, I think it helps first to define the questions. And if you're in a business there is always

What do our  
customers want?

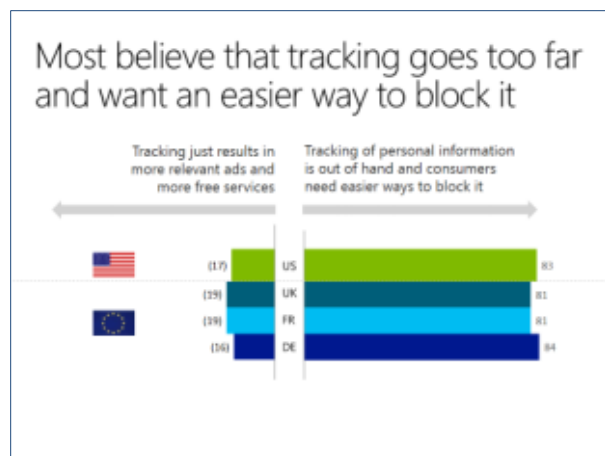
one question that you better think about very long and hard. It's this: What do our customers want?

Well, as a company we, of course, have many customers. There are times when PC manufacturers are our customers. There are times when advertisers are our customers. And we value those relationships with these companies as our customers.

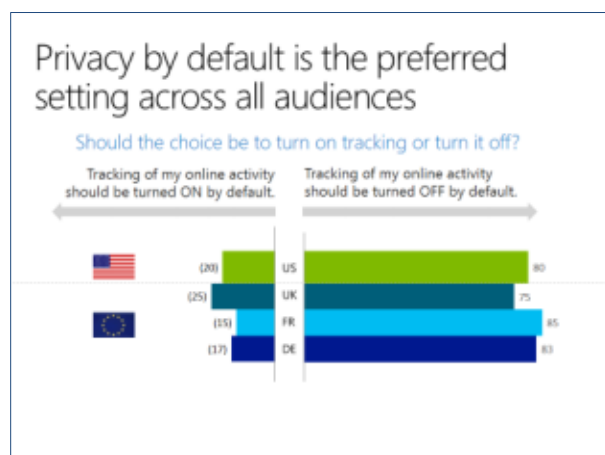
But at the end of the day, one thing is very clear: Our customers, more than any other group, are the 1 billion consumers around the world who pay us money to provide them

with cutting-edge technology. What we need to focus on is this: what do consumers want around the world?

So, after the DNT issue became a little more dramatic earlier this year, we thought it made sense to go back and see if we could learn a little bit more about what consumers want.



We commissioned some research and we asked people what they thought about these issues, and what we found in four countries – the United States, the United Kingdom, France, and Germany – is that most people today believe that online tracking goes too far, and they want an easier way to block it. In fact, in all four of these countries roughly 80 percent of consumers came down strongly on the side of wanting new steps to block the tracking of their personal information.



We also talked to people about DNT itself, and we asked them the question that we we're having to ask ourselves: Should this feature be enabled or not when they get a new browser or operating system? And what we found in all four of these countries was that 75 percent or more of the public, in fact, want this feature to be turned on, they want their privacy to be protected. They want it enabled, they want it on by default. Our votes are in, because these are the people whose needs we have to serve.

Now, of course, again we recognize that this cannot be only about one thing; we need to balance the protection of privacy with the other interests that I spoke about before. And so we've tried to give a lot of thought about where we go, and we've decided on two things.

We want to innovate and deliver new privacy benefits to consumers.

First, we want to innovate. We want to innovate and deliver new privacy benefits to consumers. We want to build on regulation and self-regulation and we want to use our research and engineering capacity to build better privacy protection into our products. That's why we believe we made the right decision when we made the decision to enable the DNT signal in the new versions of our products.



But we also recognize that we need to do more than that. If we're going to move DNT forward, let's face it: we all have a pretty steep ladder to climb, and that's going to take in our view four things, not one, to get where we all want to go.

First, we need a final and effective DNT standard that is adopted by the W3C. We need a standard that provides real privacy protection to consumers, and we need a standard that recognizes the legitimate and

reasonable needs of all participants in the ecosystem.

Second, we believe that the world of privacy will be a better place if we all recognize that browser vendors should have the ability to turn the DNT signal on or off when they ship a product. If you look at standards around the world, they specify the technology but they don't tell companies whether they have to turn it on or keep it off. That is a decision that is left to companies in the marketplace based on their assessment of the needs of their customers, and we believe that the right approach is an approach that allows vendors like Microsoft and everyone else to make this decision

But even that's not the end of the story. Third, we believe that browser vendors should clearly communicate to consumers whether the DNT signal is turned on or off and make it easy for them to change the setting. We recognize that you cannot have privacy without transparency, and we recognize that we have an obligation to ensure that it is clear to consumers how our product is configured. And there is room for an ongoing conversation across the industry and more broadly about the best ways for vendors to

communicate this information to consumers and the best ways to enable them to change this setting as they use the product themselves.

And there's a fourth and final piece as well, a piece that has gotten too little attention in our view. There needs to be an easy and effective way for responsible advertisers and ad networks to inform consumers and obtain persistent consent for their services even if the DNT signal is turned on. Just because the signal is turned on doesn't mean that a consumer wants no services that involve tracking. What it means is that consumers need to be empowered to make their own choices, and advertisers and ad networks need to be able to inform consumers in a well-understood and broadly established manner so that those ad networks that are acting responsibly can inform people and get a user's consent, even while a consumer might choose to withhold that consent from another service.

But fundamentally what the DNT signal does is empower people. It empowers people so that they're able to make that decision themselves.



When you put all of this together, whether you're talking about DNT in the narrow sense or privacy more broadly, we're reaching an important moment. We're reaching the kind of time when we can look back and say, yes, technology has changed, it's continuing to change as we meet today. But because technology has changed we can now say the needs of consumers have changed as well. The views of consumers have changed as well. The views of voters

and the public at large have changed as a result.

We need to come together. We need to grapple with those changes. We need to ensure that innovation flourishes, that the ecosystem is healthy, that technology protection is addressed. But more than anything else, we need to address the privacy needs of people around the world. We need to address the privacy needs of people and move privacy forward. That is the opportunity we have in the year ahead.





Thank you very much. (Applause.)

END