Safety, Privacy, and the Internet Paradox:
2015 and the Need for New Trans-Atlantic Rules

Brad Smith
Executive Vice President and General Counsel, Microsoft Corporation

Prepared Remarks at the Centre for European Policy Studies
Brussels, Belgium

January 20, 2015

One cannot come to Brussels on a day like today to talk about public safety, personal privacy, and the Internet without starting with a reflection on the tragic and even horrific events of recent weeks. Just as Europeans stood together with Americans in September of 2001, Americans are standing together with the French and all of Europe in January of 2015. Across the Atlantic people on both continents cherish the freedom of expression that is a hallmark not only of our societies, but of our shared traditions and past. Yet as we also have seen, without adequate public safety, this right and all of our rights are at risk.

This makes today's topic even more complex. But it also makes it even more important. More than ever, free societies need to grapple with fundamental values such as public safety and personal privacy. And the only way to do this is for us to spend the time to talk through these issues together.

2015 As a Year for Solutions. We should make no mistake, recent events should leave us all with a heightened sense of urgency: As a result, 2015 is a year that calls for solutions.

It's a year that calls for steps that will adapt laws to the technology that exists today. It's a year that calls for measures that will ensure that law enforcement can access the information it needs while people benefit from the privacy they deserve, all pursuant to proper legal process and the rule of law. It's a year that calls for governments to respect each other's borders and national sovereignty, while also enabling governments to work across borders at Internet speed under new international rules.

All of these opportunities are before us, if people can come to the table and start to work through issues that, while difficult, are definitely surmountable.

There is no better place to start, especially as we look to the international issues, than by developing new rules that can work across the Atlantic. Europe and the United States should forge a modern set of trans-Atlantic rules that will enable law enforcement to obtain information needed for lawful investigations across borders, while at the same time sustaining privacy protections for citizens and protecting free expression.

Before we get to the details, I think it helps to look at the trends of the past few years.

Since the Snowden disclosures in 2013, the world has rightly focused on revelations about governmental access to personal information. We've all learned more and thought more about when and how we want governments around the world to have access to our emails, our photos, and our text messages. This quite appropriately has also led to an even broader discussion of how private companies should use consumer information. As a company we've been calling since 2005 for comprehensive privacy legislation in the United States that would cover use of data by companies.

As 2014 unfolded, the world witnessed growing instability in Syria and Iraq, including the risk that these would lead to terrorist threats elsewhere. And as the calendar pages recently reached the end of one year and the start of a new one, we saw an unprecedented cyber-attack on Sony and then the tragic attacks in Paris.

In short, for almost 24 months, events and issues that touch safety, privacy, and the Internet have been moving forward at an accelerating pace.

Yet another facet is equally clear. While legislative debates in Europe and the United States have increasingly focused on these issues, legislation itself has not matched the pace of technological change.

To the contrary, for the most part the law has stood still.

This is the case even though most of the laws on the books literally harken from a different technological age. Here in Europe the data protection directive was written mostly in the early 1990s, when I spent seven years living and working here and using a PC that didn't have a mouse and a cell phone that couldn't be detached from my car. In the United States the Electronic Communications Privacy Act is even older, having been adopted in 1986. And while these are not the only two important laws on the books, most of the laws that are relevant to technology all share one common feature – if they were technology products, they would be in a museum.

As we begin a new year, it's time to recognize the obvious. Antiquated laws will neither keep the public safe nor privacy strong. They simply cannot, because they did not anticipate the world in which we now live.

So while on the one hand there is growing discussion of the tension between safety and privacy, we should recognize that new steps also create an opportunity to better address both of these important societal needs.

As we consider this type of opportunity, it's worth reflecting on the insights gained in just the past two months.

The Events of Recent Weeks and the Internet Paradox. Some of us at Microsoft found ourselves spending time the week before Christmas focused on whether the company would make Sony's film, "The Interview", available online. We knew that such a step would increase our own risk profile as a target for cyber-attacks. It created a hard problem, but ultimately it was not a difficult decision. Our CEO, Satya Nadella, asked engineers to spend the days before Christmas taking additional steps to prepare for such an assault. So on Christmas Eve we joined Sony and Google in announcing that we would make the film available; in our case, it was on our Xbox Live service. As we concluded, a cyber-attack on anyone's rights is a cyber-attack on everyone's rights, and the best way to deter such attacks in the future is to stand together to defend against them in the present.

In focusing on this challenge, one of the paradoxes of the Internet today became apparent. In targeting Sony, hackers used technology as a weapon to attack freedom of expression. In making Sony's film available online, Google and Microsoft used technology as a tool to defend it.

In more recent weeks this same paradox has manifested itself in ways that are even more urgent. As the world has witnessed in Paris, terrorists use technology to recruit participants, plan attacks, and proclaim credit afterwards. Law enforcement uses technology to investigate crimes – to obtain

information and analyze it to disrupt attacks before they occur. And the people of France used social media to help organize what became on the avenues of Paris the largest demonstration supporting free expression in French history.

More broadly, the Internet has become the world's principal medium for people to share ideas and communicate with each other. Like the telegraph, the telephone, and other inventions before it, people today put the Internet to use in a variety of ways – to do good and, at times, to inflict harm. This in effect defines the paradox of the Internet today. Technology is a tool. The Internet is a tool. And the good and bad uses to which this tool can be applied are limited only by people's imagination. This is true at an individual level. It's true at an organizational level. And it's true of governments and nation-states.

In short, the Internet has become the new terrain on which ideas are shared and deeds are shaped. It exists not in some sphere that is separate from the real world. Rather real people use it to advance ideas and actions that impact the real world.

The Internet and the Rule of Law. More than ever, this makes one thing abundantly clear: the Internet needs to be governed by the rule of law.

This is not a conclusion that has always been popular on the west coast of the United States or among tech companies. Yet the time has come to recognize how much things have changed.

If we're going to protect people's rights in the real world, we need to protect their rights on the Internet. If we're going to keep people safe in the real world, we need to keep them safe on the Internet. And while technology has a critical role itself in protecting people's rights and keeping people safe, technology and the Internet itself needs to be governed by law.

In other words, while the Internet must at its core remain a borderless and open and free medium, there are a certain areas where laws need to govern the real world effects of both public and private activities on the Internet. It's important to talk about what this means.

First, as we talk about our relationship across the Atlantic, this means that democratic societies, not private companies, need to decide on the balances to be struck between public values such as public safety and personal privacy. A principal challenge is that both of these goals are of huge importance in a free society. It is the type of challenge that elected representatives are uniquely positioned to address.

Especially when officials sometimes suggest that technology companies should go beyond the law and turn over to law enforcement additional information that will protect safety but compromise privacy, I think about the fact that no one elected us. If those in government want to shift the line between safety and privacy, the appropriate path is to do so by changing the law rather than asking those of us in the private sector to shift this balance by ourselves.

But it's not enough just to say that these decisions about the Internet should be made by governments. It's important to talk about how governments across the Atlantic can pursue a path to address the Internet in a way that grounds governmental action in fundamental principles around issues of privacy and free expression.

The Role of Transparency. First, reflecting our democratic traditions and principles, governments need to act with transparency. Legislatures need to pass laws, the executive branch needs to execute laws,

and courts need to enforce laws with a level of transparency that will ensure that the public is aware of what their government is doing. Some of the concerns highlighted by the Snowden disclosures go to the level of transparency in governmental actions in the United States. It wasn't always sufficiently clear to the public what the executive branch was doing. This was compounded by the degree to which the Foreign Intelligence Surveillance Court was deciding upon important interpretations of the law outside of public view. One lesson is that it's not possible to uphold democratic principles without a level of transparency that ensures the public knows what its government is doing.

This lesson is applicable not just to governments but to technology companies as well. The past two years have provided all of us with a powerful reminder. People will not use technology they do not trust. And they cannot trust technology they do not understand. Our ability to innovate therefore depends on maintaining a greater level of transparency. That's one of the reasons Microsoft, Google, and others sued the U.S. Government, insisting upon our right under the First Amendment of the Constitution to share more information with the public about the national security orders we receive. And it's why one sees so many more transparency reports published across our industry. This is a good thing, and it underscores the need for those of us in the tech sector to do more to document our own practices on how we use data.

Protecting Fundamental Freedoms. Second, those of us in the technology sector believe that governments should regulate the Internet in ways that preserve the fundamental freedoms that our customers – citizens – have long come to expect.

It's worth starting with the protection of privacy. The governments of the world recognized in the 1948 United Nations Declaration that privacy is a fundamental human right. The Council of Europe incorporated this tenet into its 1950 Convention for the Protection of Human Rights and Fundamental Freedoms. And it has remained an important part of European law ever since, including being embodied in the Charter of Fundamental Rights of the European Union.

Yet while the Internet has done so much to advance so many aspects of human progress, it has not always been so good for privacy. This week in Davos we'll talk more about the results of Microsoft's second annual worldwide poll on people's views of how personal technology is changing their lives. While people worldwide are positive about so many aspects of the Internet, 64 percent of people in developed countries believe that the Internet's impact on personal privacy has been mostly negative, an increase of 5 points compared to last year. And people are not prepared to sit back and simply watch this negative impact unfold. As the poll shows, 71 percent of people in these countries believe that current legal protections are insufficient, and 66 percent believe that the police should need a warrant or its equivalent to obtain personal information stored on a PC. Over 70 percent believe their information stored in the cloud deserves the same protection as physical files.

This all makes good sense to us. Even in this new era, if you're a consumer or you're a company, we believe that you own your e-mail, your text messages, your photos and all the content that you create. Even when you put your content in our data centers or on devices that we make, you still own it. The information you store in the cloud is entitled to the same legal protection as the information you put on paper. This means that personal information and data should not be accessed or seized without proper legal process. And this means that governments should not access the content of your private communications without probable cause – a belief that an individual is engaged in the pursuit of a crime.

Similarly, we need to continue to preserve the Internet's fundamental ability to promote education and learning and the sharing of information and ideas. While there have always been legal limits on free expression under national laws, those limits in democratic societies have typically been around the edges. The core of free expression has been to ensure that people can share ideas, even unpopular ideas, with each other. And we need to sustain this important democratic value.

Finally, as recent events have tragically made all too clear, public safety is also a paramount public need and government responsibility. Recent events have been a powerful reminder of the vital role that governments play in keeping communities safe. This means that governments have a clear need to access digital information to investigate terrorist threats and bring criminals to justice. We're committed to playing our part. When governments need access to Microsoft customer data for law enforcement or national security purposes, we work hard to quickly and appropriately respond to the legal orders served on us so that governments can get the information they need.

Yet the only way to keep the public safe, privacy secure, and free expression healthy is to ensure that all three of these values are reflected in the laws that governments write.

The Importance of Accountability. Third, as governments act to regulate the Internet, they need to do so with proper accountability. Just as technology companies need to be accountable under the law to regulators and courts, the executive branch needs to be accountable to the legislative and especially the judicial branches of governments. Balanced laws and proper judicial review need not keep law enforcement agencies from doing their job quickly. But they do need to ensure that the executive branch does its job well and with proper regard for legal process and people's rights. This is why we've advocated for reform of the Foreign Intelligence Surveillance Court in the United States. And it's why this value needs to be preserved more broadly across free societies.

Issues That Cross Borders and Respect for National Sovereignty. As we look to the year ahead, we have the opportunity to address public safety, personal privacy, and free expression not just within countries, but across borders as well. Indeed, if each country acts on its own without regard for how its laws impact borderless technology, the resulting patchwork will not serve safety, privacy, or economic advancement. As we've seen all too clearly even in recent weeks, there are times when law enforcement authorities need to access data stored in other countries. But we do not believe that the answer is to ignore national sovereignty or trample upon it. Governments need to respect each other's borders. The key instead is to strengthen the ability of governments to act pursuant to the rule of law by modernizing international law to keep pace with technology and new challenges.

The good news is that we're not working without a current legal foundation, even if it does need to be modernized. This is important for us to keep in mind, and it's a point that we've made repeatedly in our litigation against the U.S. Government in federal court in New York. We have contested a U.S. search warrant issued upon Microsoft to obtain customer emails stored in our data center in Ireland. One point we've made is that the United States has an existing Mutual Legal Assistance Treaty, or MLAT, with the Government of Ireland, and the two governments frequently cooperate closely. Indeed, in its amicus brief filed in that case, the Government of Ireland indicated it was prepared to respond expeditiously to a request for the content made pursuant to that MLAT. International cooperation, rather than unilateral intervention across borders, should be the first step that governments take when they want data that is stored somewhere else. And if existing mechanisms are inadequate, they should be improved, not ignored or simply jettisoned.

Indeed, we've seen this type of international cooperation at work in recent weeks. Just two weeks ago, the French Government sought the content of emails from two customer accounts held by Microsoft when it was in the midst of pursuing the Charlie Hebdo suspects. Rather than come to Microsoft directly in the United States, the French authorities contacted the FBI in the United States and the FBI served upon us an emergency request under a provision of the Electronic Communications Privacy Act. Despite the fact that this letter arrived electronically at 5:47 in the morning on the west coast of the United States, we were able to assess its validity under U.S. law, conclude that it was proper, pull the email content in question, and deliver it to the FBI in New York, all in exactly 45 minutes. In short, there are times, especially in emergency situations, when existing international legal processes work well. And they need to work well.

What we need, however, is new solutions that will enable the rule of law, like the Internet itself, to work well more routinely across national borders. Because while current processes sometimes work, we need to make them work better. There are two sets of steps that can be taken, and should work to take both of them this year.

Modernizing MLATs. First, we need governments to bring Mutual Legal Assistance Treaty processes into the Internet age. And there are at least two important improvements that should be relatively easy to make.

First, we should move MLATs from the age of paper and wax seals to an era of electronic communication. There is every reason for international law enforcement cooperation to move more routinely at Internet speed, as we saw the French and American authorities achieve recently. What we need are new legal processes that will enable the use of digital communications, much as we have for digital signatures for what used to be paper-based contracts.

Second, governments should standardize the terms and forms used in MLAT processes. This would enable both governments and tech companies to undertake faster legal reviews without sacrificing personal privacy. Instead of having to assess different legal terms and forms from different countries, it we could master a more concise and better standardized legal process.

In short, as this illustrates, it is possible to take steps that will better protect public safety while preserving privacy rights and respect for national sovereignty.

Towards a Bigger Step across the Atlantic. But we should not stop there. Given the importance of public safety and personal privacy, Europe and the United States should forge new trans-Atlantic legal rules that will better enable law enforcement, with appropriate safeguards, to obtain information needed for lawful investigations across borders. As I said before, there is important existing work that we can build upon. New legal rules should build on past and current examples of U.S.-European cooperation, including the Council of Europe Convention on Cybercrime and the EU-U.S. Mutual Legal Assistance Treaty. Critically, it should be built on five important principles:

(1) Direct Legal Service on Data Center Operators. First, new legal rules should enable the authorities in proper circumstances in one country to serve a new and proper order on a data center operator in another, but pursuant to legal rules that ensure respect for people's rights. These rules should require that the government issuing the order simultaneously notify the government in the country of residence of the service provider or the user, so it is aware of the law enforcement activity

that in effect is taking place within its borders or impacting one of its citizens. And it should enable either the data center operator or the receiving government to object if the order is improper.

(2) Nexus with Country Issuing the Order. Second, there should be a proper nexus between the country issuing the order and the individual whose content is being sought, and this new legal authority to obtain cloud content should be limited to specific and agreed upon criminal offenses. For physical evidence, the general rule is that the country where the evidence is located is the one with the right to obtain it, as seizing evidence is the exercise of a police power. But an agreement governing cloud content might extend this rule or focus instead on reaching the content of citizens and residents of a country, even when the content is stored in another nation. In other words, if the content of a U.S. resident is stored in Ireland, the U.S. Government could use this new legal instrument to serve a warrant directly on a data center located there. And if a French resident's content is stored in the U.S., the French Government could similarly make use of this rule to seek the content directly from a data center in the United States.

(3) Clear Standard for Issuance of an Order. Third, in order to ensure that citizens' privacy rights are respected, there should be a required minimum showing that the investigating authority must make to obtain an order requiring disclosure of content. While countries have somewhat differing legal traditions, the countries across the Atlantic share a general approach that focuses law enforcement authority on individuals who are suspected of engaging in criminal conduct. In the U.S., to obtain users' content, the law focuses on requiring "probable cause" to believe an individual has committed or possesses evidence of a specific crime. It is important to develop a minimum legal standard with which people can feel comfortable on both sides of the Atlantic.

(4) Transparency, Oversight, and Accountability. Fourth, there should be a robust system in place to ensure there is adequate oversight of governments' use of these authorities, including accountability for any misuse. Companies should have the right to publish regular and appropriate transparency reports that document the number of such orders they are receiving, the number of customer accounts that are affected, and the governments that are issuing these orders.

Orders for the most sensitive data such as email content should be issued only by a court or similar independent authority in the requesting country. An order to turn over information constitutes an infringement of privacy. It's therefore appropriate that in almost all circumstances, this fundamental right should be infringed only via an independent judgment, such a magistrate or neutral authority, that the need for the information justifies it based on the facts known at the time.

(5) Respect for Human Rights. Finally, while an agreement between Europe and the U.S. does not raise significant human rights concerns, other countries may seek to join such an accord if it proves successful. Countries should only be allowed to accede to any agreement if they meet and maintain an adequate human rights record.

In conclusion, a New Year that has highlighted the challenges of a new technology era needs to become a New Year in which we focus on new solutions. It needs to become a year in which we make more progress modernizing the laws of the past. It needs to become a year that recognizes that national laws should stop at the water's edge, but the rule of law needs to cross borders. It needs to become a year in which we recognize that, while there are tensions between safety and privacy, there are also new opportunities

for these fundamental values to move forward together. The key is to recognize that we not only have shared values but shared legal processes that can span the Atlantic. And a new legal bridge across the Atlantic can make all of this stronger.