Orit Levin's submission is the blog article below (from [1]).

Orit adds:

"The work that IETF is doing on security of Internet transmissions is timely and necessary. Recent allegations of an effort by some governments to circumvent online security measures and collect citizens' data are alarming and require a response. IETF's work on improved authentication, encryption and interoperability will help companies as the industry works to strengthen security of data online."

Protecting customer data from government snooping
4 Dec 2013 9:00 PM

The following post is from Brad Smith, General Counsel & Executive Vice President, Legal & Corporate Affairs, Microsoft.

Many of our customers have serious concerns about government surveillance of the Internet.

We share their concerns. That’s why we are taking steps to ensure governments use legal process rather than technological brute force to access customer data.

Like many others, we are especially alarmed by recent allegations in the press of a broader and concerted effort by some governments to circumvent online security measures – and in our view, legal processes and protections – in order to surreptitiously collect private customer data. In particular, recent press stories have reported allegations of governmental interception and collection – without search warrants or legal subpoenas – of customer data as it travels between customers and servers or between company data centers in our industry.

If true, these efforts threaten to seriously undermine confidence in the security and privacy of online communications. Indeed, government snooping potentially now constitutes an “advanced persistent threat,” alongside sophisticated malware and cyber attacks.

In light of these allegations, we’ve decided to take immediate and coordinated action in three areas:

· We are expanding encryption across our services.
· We are reinforcing legal protections for our customers’ data.
· We are enhancing the transparency of our software code, making it easier for customers to reassure themselves that our products do not contain back doors.

Here’s a closer look at what we’re doing:

Expanding Encryption

For many years, we’ve used encryption in our products and services to protect our customers from online criminals and hackers. While we have no direct evidence that customer data has been breached by unauthorized government access, we don't want to take any chances and are addressing this issue head on. Therefore, we will pursue a comprehensive engineering effort to strengthen the encryption of customer data across our networks and services.

This effort will include our major communications, productivity and developer services such as Outlook.com, Office 365, SkyDrive and Windows Azure, and will provide protection across the full lifecycle of customer-created content. More specifically:

· Customer content moving between our customers and Microsoft will be encrypted by default.
· All of our key platform, productivity and communications services will encrypt customer content as it moves between our data centers.
· We will use best-in-class industry cryptography to protect these channels, including Perfect Forward Secrecy and 2048-bit key lengths.
· All of this will be in place by the end of 2014, and much of it is effective immediately.
· We also will encrypt customer content that we store. In some cases, such as third-party services developed to run on Windows Azure, we’ll leave the choice to developers, but will offer the tools to allow them to easily protect data.
· We’re working with other companies across the industry to ensure that data traveling between services – from one email provider to another, for instance – is protected.

Although this is a significant engineering effort given the large number of services we offer and the hundreds of millions of customers we serve, we’re committed to moving quickly. In fact, many of our services already benefit from strong encryption in all or part of the lifecycle. For example, Office 365 and Outlook.com customer content is already encrypted when traveling between customers and Microsoft, and most Office 365 workloads as well as Windows Azure storage are now encrypted in transit

between our data centers. In other areas we’re accelerating plans to provide encryption.

Reinforcing Legal Protections

We also will take new steps to reinforce legal protections for our customers’ data. For example, we are committed to notifying business and government customers if we receive legal orders related to their data. Where a gag order attempts to prohibit us from doing this, we will challenge it in court. We’ve done this successfully in the past, and we will continue to do so in the future to preserve our ability to alert customers when governments seek to obtain their data. And we’ll assert available jurisdictional objections to legal demands when governments seek this type of customer content that is stored in another country.

Except in the most limited circumstances, we believe that government agencies can go directly to business customers or government customers for information or data about one of their employees – just as they did before these customers moved to the cloud – without undermining their investigation or national security. And when those limited circumstances arise, courts should have the opportunity to review the question and issue a decision.

Increasing Transparency

Just as we’ve called for governments to become more transparent about these issues, we believe it’s appropriate for us to be more transparent ourselves. We’re therefore taking additional steps to increase transparency by building on our long-standing program that provides government customers with an appropriate ability to review our source code, reassure themselves of its integrity, and confirm there are no back doors. We will open a network of transparency centers that will provide these customers with even greater ability to assure themselves of the integrity of Microsoft’s products. We’ll open these centers in Europe, the Americas and Asia, and we’ll further expand the range of products included in these programs.

Ultimately, we’re sensitive to the balances that must be struck when it comes to technology, security and the law. We all want to live in a world that is safe and secure, but we also want to live in a country that is protected by the Constitution. We want to ensure that important questions about government access are decided by courts rather than dictated by technological might. And we’re focused on applying new safeguards worldwide, recognizing the global nature of these issues and challenges. We believe these new steps strike the right balance, advancing for all of us both the security we need and the privacy we deserve.

[1] http://blogs.technet.com/b/microsoft_blog/archive/2013/12/04/protecting-customer-data-from-government-snooping.aspx