

Microsoft Blog Statements

# Offene Aufgaben bei der Reform staatlicher Überwachungspraktiken

Veröffentlicht von Brad Smith,  
General Counsel & Executive Vice President, Legal & Corporate Affairs, Microsoft  
16. Jun. 2014, 10:00 Uhr

Der folgende Artikel ist eine Übersetzung des von Microsoft im Blog Technet am 03.02.2014 veröffentlichten Artikels **Unfinished business on government surveillance reform**

# Offene Aufgaben bei der Reform staatlicher Überwachungspraktiken

Veröffentlicht von Brad Smith,  
General Counsel & Executive Vice President, Legal & Corporate Affairs, Microsoft  
16. Jun. 2014, 10:00 Uhr

**Im Jahr nach Auftauchen der Berichte über die Überwachungspraktiken der US-Regierung hat sich viel verändert. Es gab sogar auch erste positive Entwicklungen. Wir alle wollen in einer sicheren Welt leben, und alle Regierungen – auch die US-Regierung – spielen eine wichtige Rolle beim Schutz unseres Gemeinwesens. Aber die Realität ist auch klar: Die US-Regierung muss wichtige Hausaufgaben erledigen, um dem durch sie verursachten Vertrauensverlust in die Technologie entgegenzuwirken.**

Vor einem Jahr haben der Guardian und die Washington Post ihre ersten Berichte über das Ausmaß der Überwachung von Telefon- und Internet-Daten durch die US-Regierung, manchmal in Partnerschaft mit anderen, veröffentlicht. Im weiteren Verlauf haben wir erfahren, dass die US-Regierung nicht nur eine verhältnismäßig geringe Anzahl an Informationen über rechtliche Auskunftsanordnungen gegenüber Kommunikationsunternehmen angefordert hat. Vielmehr ist inzwischen klar, dass die Regierung Daten bei der Übertragung über das Internet abgefangen und Verknüpfungen zwischen Rechenzentren von Unternehmen ausgespäht hat. Diese Enthüllungen haben zu Recht zu einer lebhaften Debatte über das Ausmaß und die Tragweite von Überwachungsmaßnahmen durch den Staat geführt und sogar positive Veränderungen herbeigeführt. Es muss aber noch viel mehr getan werden.

Das Aufkommen von mobilen Geräten und Cloud-Services hat unser Leben in bisher nicht gekanntem Ausmaß technologisch und persönlich beeinflusst. Während einer Reise nach Europa habe ich in nahezu jedem Treffen und Gespräch erfahren, dass die Menschen konkrete Fragen und Bedenken in Bezug auf den Schutz ihrer Daten haben. Die Bedenken haben reale Auswirkungen auf die Akzeptanz der „Cloud“. Schließlich werden Menschen keine Technologie verwenden, der sie nicht vertrauen. Wir müssen eine bessere Balance zwischen Privatsphäre und nationaler Sicherheit finden, wir müssen Vertrauen wiederherstellen und dabei unsere Grundrechte verteidigen. Nach einem Jahr haben sich insbesondere fünf Themen herauskristallisiert, die die US-Regierung noch umsetzen muss:

**US-Durchsuchungsbefehle müssen auf US-Grenzen beschränkt sein:**

Die staatlichen Versuche, Durchsuchungsbeschlüsse in Bezug auf die Herausgabe von Kommunikationen von Nicht-US-Kunden, die außerhalb der USA gespeichert sind, gesetzlich zu erwirken, sind besorgniserregend. Die US-Regierung würde es ja auch nicht tolerieren, wenn andere Regierungen – ohne den Weg über US-Gerichtsverfahren zu gehen – es anstreben, Durchsuchungsbeschlüsse innerhalb der amerikanischen Staatsgrenzen zu erwirken, um den Inhalt der E-Mails von US-Bürgern an diese Regierungen zu liefern. Warum sollten andere Regierungen anders reagieren?

Die US-Regierung sollte aufhören, auf Technologie-Unternehmen Druck auszuüben, um unter Umgehung von Abkommen Zugriff auf Daten in anderen Ländern zu erlangen. Unter dem vierten Zusatzartikels („Fourth Amendment“) der Verfassung der Vereinigten Staaten hat jeder Nutzer ein Recht, seine E-Mail-Kommunikation privat zu halten. Die US-Regierung muss verfassungsrechtliche Datenschutzanforderungen wahren und die Datenschutzbestimmungen einhalten. Deshalb haben wir vor kurzem vor Gericht einen Durchsuchungsbefehl in Bezug auf in unserem Rechenzentrum in Irland gespeicherte Inhalte angefochten. Wir sind überzeugt, dass wir das Gesetz und die Verfassung der USA auf unserer Seite haben und verfolgen diesem Fall soweit und so lange wie notwendig weiter.

**Schluss mit der Massenausspähung:**

Präsident Obama äußerte den Wunsch, die massenhaften Sammlungen von Telefon-Mittschnitten zu beenden. Während Microsoft noch nie eine Aufforderung zur Massen-Sammlung von Internet-Daten erhalten hat, glauben wir, dass der USA Freedom Act verstärkt werden sollte, damit in Zukunft solche Ersuchen verboten werden.

**Reform des FISA Gerichts:**

Wir brauchen mehr Transparenz im Rahmen der Verfahren und Entscheidungen des FISA Gerichts durch die Einführung des kontradiktorischen Verfahrens als Kennzeichen eines fairen Rechtssystems. Bei Rechtsstreitigkeiten gilt: Ein Richter, der nur eine Seite einer Sache hört, kann weniger wahrscheinlich zu einem gerechten Ergebnis kommen. Der Kongress muss die Notwendigkeit einer Reform der FISA Gerichtsbarkeit erkennen und darauf reagieren.

**Verzicht auf Hacking von Datenzentren oder Kabeln:**

Unsere Bemühungen, unsere Services immer besser zu verschlüsseln, erschwert es allen Regierungen, erfolgreich Daten während der Übertragung oder im Rechenzentrum zu hacken. Sieben Monate, nachdem die Washington Post erstmals darüber berichtete, dass die National Security Agency Systeme außerhalb der USA hacken und auf Daten von Yahoo! und Google zugreifen, schweigt die Exekutive immer noch zu dieser Praxis. Sollte eine Regierung, die Ausländer, die US-Unternehmen hacken, verfolgt, nicht seine eigenen Mitarbeiter vom Eindringen in solche Unternehmen abhalten? Warum müssen wir weiter warten, bis wir eine Zusicherung zu diesem Thema bekommen?

**Mehr Transparenz:**

Vor kurzem in diesem Jahr haben wir das Recht gewonnen, Auskunft über wichtige Informationen über die Anzahl der von uns erhaltenen sicherheitsrelevanten Anfragen zu geben. Dies trägt zu einem breiteren Verständnis über das Ausmaß der Regierungsanfragen bei. Es war ein erster Schritt, aber wir glauben, dass noch weitere Details bereitgestellt werden könnten, ohne die nationale Sicherheit zu gefährden.

Während aktuell die Forderungen an die US-Regierung gerichtet werden, ist es offensichtlich, dass viele Probleme und auch Lösungen internationaler Natur sind. Wir brauchen internationale Bemühungen zur Wiederherstellung des Vertrauens der Internet-Nutzer und das richtige Gleichgewicht zwischen Datenschutz und Sicherheit. Deshalb verpflichten wir uns weiterhin für die Schaffung eines neuen internationalen Rechtsrahmens. Auf der ganzen Welt erkennen Regierungen vermehrt die Notwendigkeit für ein solches Vorhaben, und jetzt ist es an der Zeit, die Ärmel hochzukrempeln und diese voranzureiben.

Neben der Forderung von Reformen von der Regierung, sind wir als Unternehmen – auch gemeinsam mit anderen Akteuren der Branche – selbst aktiv. Dazu gehören die Erweiterung von Verschlüsselungen unsere Services, mehr Transparenz unseres Codes und die Stärkung der rechtlichen Stellung unserer Kunden, was bereits zu ersten Ergebnissen führt. Im Dezember saßen wir mit anderen Unternehmen zusammen, um zu Reformen der Überwachungspraktiken der Regierung aufzurufen. Als Ergebnis eines Rechtsstreits war es uns schließlich möglich, weitere Einzelheiten über das Volumen von Anordnungen der Regierung in Bezug auf die uns angetragene He-

rausgabe von Kundendaten zu veröffentlichen.

Trotz dieser Schritte gibt es ein Jahr nach den ersten Medienberichten noch viel zu tun. Die USA trägt die Verantwortung, hat aber auch die Chance, eine neue Vorreiterrolle einzunehmen. Es ist 225 Jahre her, dass James Madison vor dem ersten Kongress stand und die „Bill of Rights“ in den Kongress einbrachte. Dies mündete schließlich im vierten Zusatzartikel („Fourth Amendment“) unserer Verfassung. Seine Ideen gründete er auf das englische Recht und die koloniale Erfahrung, um zukünftigen Generationen das Recht zu bewahren, sich vor unzumutbaren Durchsuchungen von Seiten der Regierung zu schützen. Erklärtermaßen ist es an unserer jetzigen Generation, diesen grundlegenden Verfassungsschutz zu erhalten. Der Fortschritt der Technologie macht diese Probleme umso wichtiger. Es ist Zeit zu handeln.

Originaltext

# Unfinished business on government surveillance reform

Posted by Brad Smith,  
General Counsel & Executive Vice President, Legal & Corporate Affairs, Microsoft,  
4 Jun 2014, 11:37 AM

**In the year since news reports surfaced about U.S. government surveillance practices, a lot has changed. And there even have been some initial positive reforms. We all want to live in a safe and secure world and governments - including the U.S. government – play a vital role in helping to protect our communities. But the reality is clear. The U.S. Government needs to address important unfinished business to reduce the technology trust deficit it has created.**

In the year since news reports surfaced about U.S. government surveillance practices, a lot has changed. And there even have been some initial positive reforms. We all want to live in a safe and secure world and governments - including the U.S. government – play a vital role in helping to protect our communities. But the reality is clear. The U.S. Government needs to address important unfinished business to reduce the technology trust deficit it has created.

It was a year ago this week that the Guardian and Washington Post published their first reports about the extent of U.S. government surveillance of phone and Internet records, sometimes in partnership with others. As the story evolved, we learned that the government was not just seeking a relatively small amount of content from Internet companies via legal orders. It's now apparent that the government intercepted data

in transit across the Internet and hacked links between company data centers. These disclosures rightly have prompted a vigorous debate over the extent and scope of government surveillance, leading to some positive changes. But much more needs to be done.

With the advent of mobile devices and cloud services, technology has never been more powerful or more personal. But as I encountered in virtually every meeting during a recent trip to Europe, as well as discussions with others from around the world, people have real questions and concerns about how their data are protected. These concerns have real implications for cloud adoption. After all, people won't use technology they don't trust. We need to strike a better balance between privacy and national security to restore trust and uphold our fundamental liberties. In particular, a year on, there are



five things the U.S. government still needs to do:

**Recognize that U.S. search warrants end at U.S. borders:**

We're concerned about governmental attempts to use search warrants to force companies to turn over the contents of non-U.S. customer communications that are stored exclusively outside the United States. The U.S. government wouldn't stand for other governments seeking to serve search warrants within American borders to seize the content of U.S. citizens' emails without going through U.S. legal process. Why should it expect other governments to react any differently?

The U.S. government should stop trying to force tech companies to circumvent treaties by turning over data in other countries. Under the Fourth Amendment of the U.S. Constitution, users have a right to keep their email communications private. We need our government to uphold Constitutional privacy protections and adhere to the privacy rules established by law. That's why we recently went to court to challenge a search warrant seeking content held in our data center in Ireland. We're convinced that the law and the U.S. Constitution are on our side, and we are committed to pursuing this case as far and as long as needed.

**End bulk collection:** President Obama expressed a desire to end bulk collection of data of telephone records. While Microsoft has never received an order related to bulk collection of Internet data, we believe the USA Freedom Act should be strengthened to prohibit more clearly any such orders in the future.

**Reform the FISA Court:** We need to increase the transparency of the FISA Court's proceedings and rulings, and introduce the adversarial process that is the hallmark of a fair judicial system. There remains a fundamental truth about legal disputes: a judge who hears only one side of a case is less likely to render a just result. Congress needs to recognize and act on the need for FISA Court reform.

**Commit not to hack data centers or cables:** We believe our efforts to expand encryption across our services make it much harder for any government to successfully hack data in transit or at rest. Yet more than seven months after the Washington Post first reported that the National Security Agency hacked systems outside the U.S. to access data held by Yahoo! and Google, the Executive Branch remains silent about its views of

this practice. Shouldn't a government that prosecutes foreigners who hack into U.S. companies stop its own employees from hacking into such businesses? Why must we continue to wait for an assurance on this issue?

Continue to increase transparency: Earlier this year, we won the right to publish important data on the number of national security-related demands that we receive. This helped to provide a broader understanding of the overall volume of government orders. It was a good step, but we believe even more detail can be provided without undermining national security.

While the focus today is on the actions the U.S. government needs to take, it is clear that many of the issues and solutions to them are international in nature. We need an international effort to restore the trust of Internet users and strike the right balance between privacy and security. That's why we remain committed to the creation of new international legal frameworks. Around the world, governments are increasingly recognizing the need for such action, and now it's time for people to roll up their sleeves and pursue them.

While we continue to press the government for reforms, we've also taken actions ourselves as a company, as well as with others in the industry. These include expanding our use of encryption across our services, increasing the transparency of our code, and strengthening legal protections for customers, something that is already yielding results. In December, we came together with others in the industry to call for reforms in government surveillance practices, and as a result of litigation, we were able to publish additional details about the volume of national security orders for customer data we receive from the US government.

Despite these steps, a year after the first news reports, there is much more to do. The U.S. has both a responsibility and an opportunity to show new leadership on these issues. It was 225 years ago this Sunday that James Madison stood up in the first Congress and proposed the Bill of Rights, including what became the Fourth Amendment to our Constitution. He built on English law and colonial experience to preserve for future generations the right of people to be secure from unreasonable government searches. But by definition it is up to our own generation to preserve this fundamental constitutional protection. The advance of technology makes these issues even more important. Now is the time to act.

Editor's note: On May 19, Brad Smith addressed the need for additional government surveillance reforms and ways that government and corporations can address peoples' desires for better transparency, control and accountability when it comes to their data. Video highlights are available below.

**Originalpost**

<http://blogs.microsoft.com/on-the-issues/2014/06/04/unfinished-business-on-government-surveillance-reform/>