Microsoft

Microsoft Blog Statements

Zum Umgang mit rechtmäßigen Anfragen der Regierung nach Kundendaten

Veröffentlicht von Brad Smith,
General Counsel & Executive Vice President, Legal & Corporate Affairs, Microsoft
16. Juli 2013, 12.08 Uhr

Der folgende Artikel ist eine Übersetzung des von Microsoft im Blog Technet am 16.07.2013 veröffentlichten Artikels
Responding Government Legal demands for customer Data

Zum Umgang mit rechtmäßigen Anfragen der Regierung nach Kundendaten

Veröffentlicht von Brad Smith,
General Counsel & Executive Vice President, Legal & Corporate Affairs, Microsoft
16. Juli 2013, 12.08 Uhr

Heute haben wir den Attorney General (Generalbundesanwalt) der Vereinigten Staaten gebeten, dass er persönlich Maßnahmen ergreift, die es Microsoft und anderen Unternehmen erlauben, der Öffentlichkeit vollständigere Informationen darüber mitzuteilen, wie wir mit nationalen Sicherheitsanfragen zu Kundeninformationen umgehen.

Wir sind der Auffassung, dass die US-Verfassung uns die Freiheit gewährt, der Öffentlichkeit mehr Informationen mitzuteilen, allerdings hält uns die Regierung davon ab. Beispielsweise haben Anwälte der Regierung noch nicht auf den von uns am 19. Juni bei Gericht eingereichten Antrag reagiert, in dem wir um Erlaubnis bitten, den Umfang der an uns gerichteten nationalen Sicherheitsanfragen zu veröffentlichen. Wir hoffen, dass der Attorney General einschreitet, um diese Situation zu ändern.

Bis dahin wollen wir so viele Informationen wie zurzeit möglich mitteilen. Die Interpretation der durchgesickerten Regierungsdokumente, über die in der letzten Woche in den Medien berichtet wurde, enthalten bedeutende Ungenauigkeiten.

Wir haben die Regierung erneut um Erlaubnis gebeten, die Themen zu diskutieren, die durch diese neuen Dokumente aufgeworfen wurden, und unsere Anfrage wurde von den Anwälten der Regierung abgelehnt. In der Zwischenzeit haben wir die untenstehenden Informationen zusammengestellt, die wir Ihnen als Reaktion auf die Behauptungen in der Berichterstattung mitteilen können:

Outlook.com (ehemals Hotmail):
Wir stellen Regierungen keinen direkten Zugang zu E-Mails oder Sofortnachrichten zur Verfügung. Punkt. Wie alle Anbieter von Kommunikationsdiensten sind wir zuweilen verpflichtet, aufgrund eines Durchsuchungsbefehls oder einer gerichtlichen Verfügung den gesetzlich zulässigen Forderungen von Regierungen zur Übergabe von Inhalten bestimmter Konten zu entsprechen. Dies gilt für die USA und andere Länder, in denen wir Daten speichern. Wenn wir eine solche Anforderung erhalten, überprüfen wir sie und entsprechen ihr, wenn wir dazu verpflichtet sind. Wir statten keine Regierung mit den technischen Möglichkeiten aus, auf Nutzerinhalt direkt oder selbstständig zuzugreifen. Stattdessen sind Regierungen weiterhin auf den Rechtsweg angewiesen, wenn sie von uns bestimmte Informationen über kenntlich gemachte Konten einholen möchten.

Es überrascht nicht, dass wir diesen Arten von rechtlichen Verpflichtungen auch dann noch unterliegen, wenn wir unsere Produkte aktualisieren, die Verschlüsselung und die Sicherheitsmaßnahmen verstärken, um die Inhalte auf ihrem Weg durch das Netz besser zu schützen. Die kürzlich durchgesickerten Regierungsdokumente haben die Hinzufügung der HTTPS-Verschlüsselung für Outlook.com-Sofortnachrichten im Focus, die derart ausgelegt ist, die Inhalte auf ihrem Weg durch das Internet sicherer zu machen. Zur Klarstellung: Wir ermöglichen es keiner Regierung, die Verschlüsselung zu knacken, noch stellen wir der Regierung Chiffrierschlüssel zur Verfügung. Wenn wir rechtlich dazu verpflichtet sind, Anforderungen zu entsprechen, entnehmen wir den spezifizierten Inhalt unseren Servern, wo er in einem unverschlüsselten Zustand hinterlegt ist, und stellen ihn dann der Regierungsbehörde zur Verfügung.

Ohne näher auf die technischen Einzelheiten einzugehen, laufen sämtliche der neusten durchgesickerten Dokumente auf zwei Dinge hinaus. Erstens haben wir zwar mit der Regierung, wie letzte Woche berichtet, über die Notwendigkeit der Einhaltung von Rechtsvorschriften gesprochen, jedoch hat Microsoft in keinem dieser Gespräche einer Regierung direkten Zugang zu Nutzerinhalt oder das Knacken unserer Verschlüsselung ermöglicht oder vereinbart, dies in Zukunft zu tun. Zweitens ging es in diesen Gesprächen stattdessen darum, wie Microsoft der weiterhin bestehenden Verpflichtung zur Einhaltung von Rechtsvorschriften nachkommt, indem als Reaktion auf rechtmäßige Verfügungen der Regierung bestimmte Informationen zur Verfügung gestellt werden.

SkyDrive:
Wir reagieren in derselben Art und Weise auf rechtmäßige Anforderungen der Regierung von in SkyDrive gespeicherten Daten. Alle Anbieter dieser Arten von Speicherdiensten haben schon immer der rechtlichen Verpflichtung unterlegen, gespeicherte Inhalte zur Verfügung zu stellen, wenn sie ordnungsgemäße, rechtmäßige Anforderungen erhalten. 2013 haben wir Änderungen bei unseren Verfahren vorgenommen, um der steigenden Anzahl von rechtmäßigen Forderungen von Regierungen weltweit weiterhin entsprechen zu können. Keine dieser Änderungen hat es einer Regierung ermöglicht, direkt auf SkyDrive zuzugreifen. Auch hat keine dieser Änderungen etwas an der Tatsache geändert, dass wir weiterhin von Regierungen verlangen, den Rechtsweg zu beschreiten, wenn sie Kundendaten anfragen. Der Prozess für die Herausgabe von SkyDrive-Dateien ist derselbe, gleich, ob es um einen strafrechtlichen Durchsuchungsbefehl geht oder um die Reaktion auf eine nationale Sicherheitsverfügung, ob in den USA oder anderswo.

Skype-Anrufe:
Wie auch bei anderen Diensten regieren wir nur auf rechtmäßige Anforderungen einer Regierung und wir entsprechen nur Verfügungen mit Anfragen zu bestimmten Konten oder Kennungen. Die Berichterstattung von letzter Woche beinhaltet Behauptungen über eine bestimmte Änderung im Jahr 2012. Wir arbeiten weiterhin an einer Optimierung und Weiterentwicklung der Skype-Angebote und haben für Skype eine Reihe von Verbesserungen im Back-End-Bereich vorgenommen, wie beispielsweise im Jahr 2012, als das Hosting von Netzwerkknoten (supernodes) von extern nach intern verlegt wurde und ein Großteil des Sofortnachrichten-Verkehrs von Skype auf Server in unseren Datenzentren verlagert wurde. Diese Änderungen wurden nicht vorgenommen, um einen verstärkten staatlichen Zugang zu Audio-, Video-, Nachrichten- oder anderen Kundendaten zu ermöglichen. Mit Blick auf die Zukunft, in der internetbasierte Sprach- und Videokommunikation zunehmen wird, wird deutlich, dass Regierungen ein Interesse an der Ausübung (bzw. Schaffung) rechtlicher Befugnisse zur Sicherung des Zugriffs auf diese Art von Inhalt haben werden, um Ermittlungen bei Verbrechen anzustellen oder Terrorismus zu bekämpfen. Wir vermuten daher, dass sämtliche Anrufe, ob sie über das Internet, Festnetz oder Mobiltelefon getätigt werden, ein ähnliches Niveau an Privatsphäre und Sicherheit anbieten werden. Selbst unter diesen Umständen bleibt Microsoft dabei, nur auf gültige, rechtmäßige Anfragen zu bestimmten Nutzerkonteninformationen zu antworten. Wir werden Regierungen keinen direkten oder uneingeschränkten Zugriff auf Kundendaten oder Chiffrierschlüssel zur Verfügung stellen.

Geschäfts-E-Mails und Speicherung von Dokumenten:
Wenn wir eine Anforderung der Regierung zu Daten von Geschäftskunden erhalten, unternehmen wir Schritte, um die Regierung direkt an den Kunden weiterzuleiten, und wir informieren den Kunden, es sei denn, dass uns dies gesetzlich verboten ist. Wir haben einer Regierung nie Kundendaten von einem unserer Geschäfts- oder Regierungskunden für Zwecke

der nationalen Sicherheit zur Verfügung gestellt. Hinsichtlich der Anfragen zur Strafverfolgung haben wir in unserem Bericht zu Anfragen zur Strafverfolgung deutlich gemacht, dass wir 2012 nur vier Anfragen im Hinblick auf Geschäfts- oder Regierungskunden entsprochen haben. In drei Fällen haben wir die Kunden über die Anforderung informiert und sie haben uns gebeten, die Daten zu übermitteln. Im vierten Fall hat der Kunde die Forderung direkt erhalten und Microsoft gebeten, die Daten zu übermitteln. Wir ermöglichen es keiner Regierung, die zwischen unseren Geschäftskunden und ihren Daten in der Cloud genutzte Verschlüsselung zu knacken, noch stellen wir der Regierung die Chiffrierschlüssel zur Verfügung.

Zusammengefasst:
Wenn Regierungen von Microsoft Informationen in Bezug auf Kunden einholen wollen, streben wir danach, unseren Grundsätzen zu entsprechen – den Umfang von Offenlegungen zu beschränken und der Transparenz verpflichtet zu sein. Nach alledem gilt das Folgende für alle unserer Software- und Dienstleistungs-Angebote:

- **Microsoft stellt keiner Regierung direkten bzw. uneingeschränkten Zugang zu den Daten unserer Kunden zur Verfügung. Microsoft zieht und übermittelt nur die Daten, die in der betreffenden rechtmäßigen Forderung angeordnet wurden.**

- **Wenn eine Regierung Kundendaten haben möchte – auch für Zwecke der nationalen Sicherheit – muss sie den einschlägigen Rechtsweg folgen, was bedeutet, dass sie uns eine gerichtliche Verfügung über die Inhalte oder eine Zwangsherausgabe für Kontoinformationen zustellt.**

- **Wir reagieren nur auf Anfragen zu bestimmten Konten oder Kennungen. Es gibt keinen pauschalen oder willkürlichen Zugriff auf Kundendaten von Microsoft. Die angesammelten Daten, die wir veröffentlichen konnten, zeigen deutlich, dass nur ein sehr kleiner Teil – Bruchteile eines Prozents – unserer Kunden je Gegenstand einer Anforderung der Regierung in Bezug auf Strafrecht oder nationale Sicherheit waren.**

- **Sämtliche dieser Anfragen werden ausdrücklich von dem Compliance-Team von Microsoft überprüft, das die Gültigkeit der Anfragen sicherstellt, die ungültigen ablehnt und dafür Sorge trägt, dass wir nur die in der Verfügung angegebenen Daten zur Verfügung stellen. Während wir zur Entsprechung verpflichtet sind, bewältigen wir weiterhin den Compliance-Prozess, indem wir die bei uns eingegangenen Verfügungen verfolgen, ihre Gültigkeit sicherstellen und nur die in der Verfügung abgedeckten Daten offengelegen.**

- **Microsoft ist verpflichtet, den anwendbaren Gesetzen zu entsprechen, die Regierungen rund um den Globus – nicht nur in den USA – verabschieden, und dies beinhaltet die Beantwortung von rechtmäßige Anforderungen von Kundendaten. Wir leben alle in einer Welt, in der Unternehmen und Regierungsbehörden große Datenvolumina verwenden und es wäre ein Fehler, anzunehmen, dass dies nur für die USA gilt. Behörden erhalten diese Informationen wahrscheinlich aus einer Vielzahl von Quellen und auf vielfältige Art und Weise, aber wenn sie Kundendaten von Microsoft einholen wollen, müssen sie den Rechtsweg einhalten.**

Die Welt braucht eine offenere und öffentliche Debatte über diese Praktiken. Während sich die Debatte auf die Praktiken sämtlicher Regierungen fokussieren sollte, sollte sie bei den Praktiken in den USA beginnen. Teilweise ist dies eine der offensichtlichen Folgen der neuesten Berichte in den Nachrichten, aber es geht darüber hinaus und handelt sich um etwas Zeitloseres. Die USA hat Vorbildcharakter durch Gewährung des verfassungsmäßigen Rechts auf freie Meinungsäußerung. Wir wollen dieses Recht ausüben. Da uns die Anwälte der Regierung davon abhalten, der Öffentlichkeit mehr Informationen mitzuteilen, brauchen wir zur Aufrechterhaltung der Verfassung den Attorney General.

Wenn wir eine Genehmigung zur Mitteilung von mehr Informationen erhalten, werden wir sie unverzüglich veröffentlichen.

Originaltext

Responding government legal demands for customer data

Posted by Brad Smith,
General Counsel & Executive Vice President, Legal & Corporate Affairs, Microsoft,
16. Jul 2013, 12.08 PM

Today we have asked the Attorney General of the United States to personally take action to permit Microsoft and other companies to share publicly more complete information about how we handle national security requests for customer information.

We believe the U.S. Constitution guarantees our freedom to share more information with the public, yet the Government is stopping us. For example, Government lawyers have yet to respond to the petition we filed in court on June 19, seeking permission to publish the volume of national security requests we have received. We hope the Attorney General can step in to change this situation.

Until that happens, we want to share as much information as we currently can. There are significant inaccuracies in the interpretations of leaked government documents reported in the media last week. We have asked the Government again for permission to discuss the issues raised by these new documents, and our request was denied by government lawyers. In the meantime, we have summarized below the information that we are in a position to share, in response to the allegations in the reporting:

Outlook.com (formerly Hotmail):
We do not provide any government with direct access to emails or instant messages. Full stop. Like all providers of communications services, we are sometimes obligated to comply with lawful demands from governments to turn over content for specific accounts, pursuant to a search warrant or court order. This is true in the United States and other countries where we store data. When we receive such a demand, we review it and, if obligated to we comply. We do not provide any government with the technical capability to access user content directly or by itself. Instead, governments must continue to rely on legal process to seek from us specified information about identified accounts.

Not surprisingly, we remain subject to these types of legal obligations when we update our products and even when we strengthen encryption and security measures to better protect content as it travels across the Web. Recent leaked government documents have focused on the addition of HTTPS encryption to Outlook.com instant messaging, which is designed to make this content more secure as it travels across the Internet. To be clear, we do not provide any government with the ability to break the encryption, nor do we provide the government with the encryption keys. When we are legally obligated to comply with demands, we pull the specified content from our servers where it sits in an unencrypted state, and then we provide it to the government agency.

Cutting through the technical details, all of the information in the recent leaked government documents adds up to two things. First, while we did discuss legal compliance requirements with the government as reported last week, in none of these discussions did Microsoft provide or agree to provide

any government with direct access to user content or the ability to break our encryption. Second, these discussions were instead about how Microsoft would meet its continuing obligation to comply with the law by providing specific information in response to lawful government orders.

SkyDrive:

We respond to legal government demands for data stored in SkyDrive in the same way. All providers of these types of storage services have always been under legal obligations to provide stored content when they receive proper legal demands. In 2013 we made changes to our processes to be able to continue to comply with an increasing number of legal demands of governments worldwide. None of these changes provided any government with direct access to SkyDrive. Nor did any of them change the fact that we still require governments to follow legal processes when requesting customer data. The process used for producing SkyDrive files is the same whether it is for a criminal search warrant or in response to a national security order, in the United States or elsewhere.

Skype Calls:

As with other services, we only respond to legal government demands, and we only comply with orders for requests about specific accounts or identifiers. The reporting last week made allegations about a specific change in 2012. We continue to enhance and evolve the Skype offerings and have made a number of improvements to the technical back-end for Skype, such as the 2012 move to in-house hosting of "supernodes" and the migration of much Skype IM traffic to servers in our data centers. These changes were not made to facilitate greater government access to audio, video, messaging or other customer data. Looking forward, as Internet-based voice and video communications increase, it is clear that governments will have an interest in using (or establishing) legal powers to secure access to this kind of content to investigate crimes or tackle terrorism. We therefore assume that all calls, whether over the Internet or by fixed line or mobile phone, will offer similar levels of privacy and security. Even in these circumstances Microsoft remains committed to responding only to valid legal demands for specific user account information. We will not provide governments with direct or unfettered access to customer data or encryption keys.

Enterprise Email and Document Storage:

If we receive a government demand for data held by a business customer, we take steps to redirect the government to the customer directly, and we notify the customer unless we are legally prohibited from doing so. We have never provided any government with customer data from any of our business or government customers for national security purposes. In terms of criminal law enforcement requests, we made clear in our Law Enforcement Requests Report that throughout 2012 we only complied with four requests related to business or government customers. In three instances, we notified the customer of the demand and they asked us to produce the data. In the fourth case, the customer received the demand directly and asked Microsoft to produce the data. We do not provide any government with the ability to break the encryption used between our business customers and their data in the cloud, nor do we provide the government with the encryption keys.

In short

In short, when governments seek information from Microsoft relating to customers, we strive to be principled, limited in what we disclose, and committed to transparency. Put together, all of this adds up to the following across all of our software and services:

- **Microsoft does not provide any government with direct and unfettered access to our customer's data. Microsoft only pulls and then provides the specific data mandated by the relevant legal demand.**

- **If a government wants customer data – including for national security purposes – it needs to follow applicable legal process, meaning it must serve us with a court order for content or subpoena for account information.**

- **We only respond to requests for specific accounts and identifiers. There is no blanket or indiscriminate access to Microsoft's customer data. The aggregate data we have been able to publish shows clearly that only a tiny fraction – fractions of a percent – of our customers have ever been subject to a government demand related to criminal law or national security.**

- **All of these requests are explicitly reviewed by Micro-**

soft's compliance team, who ensure the requests are valid, reject those that are not, and make sure we only provide the data specified in the order. While we are obligated to comply, we continue to manage the compliance process by keeping track of the orders received, ensuring they are valid, and disclosing only the data covered by the order.

- Microsoft is obligated to comply with the applicable laws that governments around the world – not just the United States – pass, and this includes responding to legal demands for customer data. All of us now live in a world in which companies and government agencies are using big data, and it would be a mistake to assume this somehow is confined to the United States. Agencies likely obtain this information from a variety of sources and in a variety of ways, but if they seek customer data from Microsoft they must follow legal processes.

The world needs a more open and public discussion of these practices. While the debate should focus on the practices of all governments, it should start with practices in the United States. In part, this is an obvious reflection of the most recent stories in the news. It's also a reflection of something more timeless. The United States has been a role model by guaranteeing a Constitutional right to free speech. We want to exercise that right. With U.S. Government lawyers stopping us from sharing more information with the public, we need the Attorney General to uphold the Constitution.

If we do receive approval to share more information, we'll publish it immediately.

Originalpost:
http://blogs.microsoft.com/on-the-issues/2013/07/16/responding-to-government-legal-demands-for-customer-data/