Microsoft

Microsoft's Law Enforcement Requests Report for the first six months of 2013

This is our second Law Enforcement Requests Report and it covers the period from January to June 2013.

The report details the number of requests for data we received from law enforcement agencies around the world, and how Microsoft responds to those requests. It covers requests for data relating to all of Microsoft's online and cloud services, including Skype.

Unfortunately, we are not currently permitted to report detailed information about the type and volume of any national security orders (e.g. FISA Orders and FISA Directives) that we may receive **so any national security orders we may receive are not included in this report**. We have summarized, per government direction, the aggregate volume of National Security Letters we have received.

What does the data show?

- Microsoft (including Skype) received 37,196 requests from law enforcement agencies potentially impacting 66,539 accounts in the first six months of this year. This compares to 75,378 requests and 137,424 potential accounts in the whole of 2012.
- Approximately 77 percent of requests resulted in the disclosure of "non-content data". No data at all was disclosed in nearly 21 percent of requests.
- Only a small number of requests result in the disclosure of customer content data, just 2.19 percent of total requests. 92 percent of the requests that resulted in the disclosure of customer content were from United States law enforcement agencies. This is again, broadly in line with what we saw in 2012.
- As with the 2012 report this new data shows that across our services only a tiny fraction of accounts, less that 0.01 percent are ever affected by law enforcement requests for customer data. Of the small number that were affected, the overwhelming majority involved the disclosure of non-content data.
- While we see requests from a large number of countries, when you look at the number of overall number, the requests are fairly concentrated with over 73% of requests coming from five countries, the United States, Turkey, Germany, the United Kingdom, and France. For Skype the requests were similarly concentrated, with four countries, the US, UK, France and Germany, accounting for over 70 percent of requests.
- Law enforcement sought information about only a tiny fraction of the millions of end users of our enterprise services, such as Office 365. We received 19 requests for e-mail accounts we host for enterprise customers, seeking information about 48 accounts. We disclosed customer data in response to five of those requests (4 content; 1 only non-content), and in all but one case, we were able to notify the customer. We rejected the request, found no responsive data, or redirected law enforcement to obtain the information from the customer directly in thirteen of those cases. One request is still pending.
- For all 19 enterprise requests, the legal demands were from law enforcement entities located in the U.S., and sought data about accounts associated with enterprise customers located in the United States. In addition, to date, Microsoft has not disclosed enterprise customer data in response to a government request issued pursuant to national security laws.

As we said in our first Law Enforcement Requests Report, we've tried to provide the data in a way that is helpful to the community, both in terms of what we report and making it available for download and

detailed review. As promised, we've also aligned the reporting for Skype to be consistent with the rest of Microsoft, and over time as Microsoft's services are integrated more closely we'll fully integrate reporting.

We believe this data is valuable and useful to the community that is looking to better understand these issues. However we recognize that this report—focused on law enforcement and excluding national security—only paints part of the picture. We believe the U.S. Constitution guarantees our freedom to share more information with you and are therefore are currently petitioning the federal government for permission to publish more detailed data relating to any legal demands we may have received from the U.S. pursuant to the Foreign Intelligence Surveillance Act (FISA).

In June we published aggregate data which showed the combined totals of all requests from US government agencies for the second half of 2012, including if we received them, national security orders. While we believe that had some value in *quantifying the overall volume of requests we received*, it is clear that the continued lack of transparency makes it very difficult for the community—including the global community—to have an informed debate about the balance between investigating crimes, keeping communities safe, and personal privacy.

Microsoft remains committed to respecting human rights, free expression, and individual privacy. We seek to operate all of the services we own in a manner that's consistent with our Global Human Rights Statement and responsibilities as a member of the Global Network Initiative. We strive to adopt practices that are clear and straightforward and have provided additional detail on our policies and practices for responding to law enforcement requests for customer data in our FAQs accompanying this report. For additional information about how we use and protect customer information, please read the Microsoft Online Privacy Statement and the Skype Privacy Policy.

Combined Microsoft Services (including Skype): January - June 2013 Law Enforcement Requests Report

Country	Total Number of Law Enforcement Requests	Accounts/Users Specified in Requests	Some Customer Data Disclosed				No Customer Data Disclosed			
			Law Enforcement Requests Resulting in Disclosure of Content		Law Enforcement Requests Resulting in Disclosure of Only Subscriber/Transactional (Non-Content) Data		Law Enforcement Requests Resulting in Disclosure of No Customer Data (No Data Found)		Law Enforcement Requests Resulting in Disclosure of No Customer Data(Request Rejected for Not Meeting Legal Requirements)	
			%	#	%	#	%	#	%	#
TOTAL	**37,196**	**66,539**	**2.2%**	817	**77.2%**	28,698	**18.2%**	6,769	**2.4%**	911
Argentina	**455**	**675**	**0.0%**	-	**81.5%**	371	**16.5%**	75	**2.0%**	9
Australia	**1,219**	**1,462**	**0.0%**	-	**86.1%**	1,050	**13.4%**	163	**0.5%**	6
Austria	**9**	**15**	**0.0%**	-	**77.8%**	7	**11.1%**	1	**11.1%**	1
Belarus	**1**	**1**	**0.0%**	-	**100.0%**	1	**0.0%**	-	**0.0%**	-
Belgium	**500**	**784**	**0.0%**	-	**81.2%**	406	**18.8%**	94	**0.0%**	-
Brazil	**1,098**	**2,019**	**5.8%**	64	**70.9%**	778	**22.7%**	249	**0.6%**	7
British Virgin Islands	**1**	**1**	**0.0%**	-	**100.0%**	1	**0.0%**	-	**0.0%**	-
Bulgaria	**2**	**4**	**0.0%**	-	**100.0%**	2	**0.0%**	-	**0.0%**	-
Canada	**69**	**200**	**4.3%**	3	**81.2%**	56	**7.2%**	5	**7.2%**	5
Chile	**204**	**292**	**0.0%**	-	**84.3%**	172	**15.2%**	31	**0.5%**	1
China	**3**	**42**	**0.0%**	-	**100.0%**	3	**0.0%**	-	**0.0%**	-
Colombia	**97**	**170**	**0.0%**	-	**86.6%**	84	**11.3%**	11	**2.1%**	2
Costa Rica	**48**	**61**	**0.0%**	-	**89.6%**	43	**10.4%**	5	**0.0%**	-
Czech Republic	**34**	**62**	**0.0%**	-	**76.5%**	26	**11.8%**	4	**11.8%**	4
Denmark	**107**	**256**	**0.0%**	-	**83.2%**	89	**15.9%**	17	**0.9%**	1
Dominican Republic	**7**	**79**	**0.0%**	-	**100.0%**	7	**0.0%**	-	**0.0%**	-
Ecuador	**17**	**18**	**0.0%**	-	**100.0%**	17	**0.0%**	-	**0.0%**	-
El Salvador	**9**	**15**	**0.0%**	-	**100.0%**	9	**0.0%**	-	**0.0%**	-
Estonia	**3**	**6**	**0.0%**	-	**100.0%**	3	**0.0%**	-	**0.0%**	-
Finland	**29**	**48**	**0.0%**	-	**86.2%**	25	**13.8%**	4	**0.0%**	-
France	**4,379**	**7,926**	**0.0%**	-	**82.2%**	3,599	**17.0%**	744	**0.8%**	36
French Polynesia	**1**	**1**	**0.0%**	-	**100.0%**	1	**0.0%**	-	**0.0%**	-
French Southern Territories	**1**	**1**	**0.0%**	-	**0.0%**	-	**100.0%**	1	**0.0%**	-
Germany	**5,185**	**9,670**	**0.0%**	-	**83.3%**	4,318	**15.9%**	826	**0.8%**	41
Greece	**10**	**64**	**0.0%**	-	**90.0%**	9	**10.0%**	1	**0.0%**	-
Hong Kong	**597**	**597**	**0.0%**	-	**83.9%**	501	**16.1%**	96	**0.0%**	-
Hungary	**70**	**127**	**0.0%**	-	**82.9%**	58	**15.7%**	11	**1.4%**	1
Iceland	**6**	**7**	**0.0%**	-	**83.3%**	5	**16.7%**	1	**0.0%**	-
India	**278**	**413**	**0.0%**	-	**80.6%**	224	**16.2%**	45	**3.2%**	9
Ireland	**40**	**69**	**2.5%**	1	**47.5%**	19	**32.5%**	13	**17.5%**	7
Israel	**34**	**66**	**0.0%**	-	**73.5%**	25	**8.8%**	3	**17.6%**	6
Italy	**852**	**1,172**	**0.0%**	-	**78.2%**	666	**18.9%**	161	**2.9%**	25
Japan	**476**	**574**	**0.0%**	-	**79.2%**	377	**13.4%**	64	**7.4%**	35
Korea	**126**	**222**	**0.0%**	-	**86.5%**	109	**11.9%**	15	**1.6%**	2
Latvia	**1**	**1**	**0.0%**	-	**100.0%**	1	**0.0%**	-	**0.0%**	-
Lithuania	**6**	**20**	**0.0%**	-	**50.0%**	3	**16.7%**	1	**33.3%**	2
Luxembourg	**55**	**121**	**0.0%**	-	**78.2%**	43	**21.8%**	12	**0.0%**	-
Malta	**29**	**34**	**0.0%**	-	**82.8%**	24	**17.2%**	5	**0.0%**	-
Mexico	**340**	**770**	**0.0%**	-	**85.0%**	289	**14.7%**	50	**0.3%**	1
Moldova	**1**	**2**	**0.0%**	-	**100.0%**	1	**0.0%**	-	**0.0%**	-
Monaco	**2**	**2**	**0.0%**	-	**50.0%**	1	**0.0%**	-	**50.0%**	1
Netherlands	**411**	**714**	**0.0%**	-	**78.1%**	321	**21.7%**	89	**0.2%**	1
New Zealand	**34**	**43**	**0.0%**	-	**82.4%**	28	**11.8%**	4	**5.9%**	2
Norway	**74**	**131**	**0.0%**	-	**83.8%**	62	**16.2%**	12	**0.0%**	-
Panama	**10**	**18**	**0.0%**	-	**90.0%**	9	**10.0%**	1	**0.0%**	-
Peru	**29**	**77**	**0.0%**	-	**93.1%**	27	**6.9%**	2	**0.0%**	-
Poland	**55**	**76**	**0.0%**	-	**72.7%**	40	**25.5%**	14	**1.8%**	1
Portugal	**334**	**411**	**0.0%**	-	**81.7%**	273	**18.3%**	61	**0.0%**	-
Qatar	**1**	**1**	**0.0%**	-	**100.0%**	1	**0.0%**	-	**0.0%**	-
Russian Federation	**3**	**6**	**0.0%**	-	**100.0%**	3	**0.0%**	-	**0.0%**	-
Singapore	**66**	**92**	**0.0%**	-	**90.9%**	60	**9.1%**	6	**0.0%**	-
Slovakia	**15**	**18**	**0.0%**	-	**93.3%**	14	**0.0%**	-	**6.7%**	1
Spain	**927**	**1,478**	**0.0%**	-	**79.3%**	735	**20.2%**	187	**0.5%**	5

Sweden	**281**	**825**	**0.0%**	-	**87.5%**	246	**10.3%**	29	**2.1%**	6
Switzerland	**43**	**80**	**0.0%**	-	**62.8%**	27	**25.6%**	11	**11.6%**	5
Taiwan	**802**	**1,516**	**0.0%**	-	**85.5%**	686	**14.2%**	114	**0.2%**	2
Thailand	**44**	**56**	**0.0%**	-	**84.1%**	37	**15.9%**	7	**0.0%**	-
Trinidad and Tobago	**1**	**2**	**0.0%**	-	**100.0%**	1	**0.0%**	-	**0.0%**	-
Turkey	**6,226**	**7,333**	**0.0%**	-	**75.1%**	4,674	**24.9%**	1,549	**0.0%**	3
Ukraine	**5**	**32**	**0.0%**	-	**80.0%**	4	**20.0%**	1	**0.0%**	-
United Kingdom	**4,404**	**6,723**	**0.0%**	-	**78.2%**	3,443	**19.7%**	867	**2.1%**	94
United States	**7,014**	**18,809**	**10.7%**	749	**65.1%**	4,569	**15.8%**	1,107	**8.4%**	588
Uruguay	**1**	**1**	**0.0%**	-	**100.0%**	1	**0.0%**	-	**0.0%**	-
Venezuala	**15**	**28**	**0.0%**	-	**93.3%**	14	**0.0%**	-	**6.7%**	1

Skype: January - June 2013 Law Enforcement Requests Report

Country	Total Number of Law Enforcement Requests	Accounts/Users Specified in Requests	Some Customer Data Disclosed				No Customer Data Disclosed			
			Law Enforcement Requests Resulting in Disclosure of Content		Law Enforcement Requests Resulting in Disclosure of Only Subscriber/Transactional (Non-Content) Data		Law Enforcement Requests Resulting in Disclosure of No Customer Data (No Data Found)		Law Enforcement Requests Resulting in Disclosure of No Customer Data(Request Rejected for Not Meeting Legal Requirements)	
			%	#	%	#	%	#	%	#
TOTAL	**3,509**	**10,585**	**0.0%**	**-**	**82.4%**	**2,891**	**10.3%**	**361**	**7.3%**	**257**
Argentina	**12**	**19**	**0.0%**	-	**25.0%**	3	**0.0%**	-	**75.0%**	9
Australia	**197**	**266**	**0.0%**	-	**87.8%**	173	**10.7%**	21	**1.5%**	3
Austria	**9**	**15**	**0.0%**	-	**77.8%**	7	**11.1%**	1	**11.1%**	1
Belarus	**1**	**1**	**0.0%**	-	**100.0%**	1	**0.0%**	-	**0.0%**	-
Belgium	**27**	**120**	**0.0%**	-	**81.5%**	22	**18.5%**	5	**0.0%**	-
Brazil	**5**	**6**	**0.0%**	-	**60.0%**	3	**20.0%**	1	**20.0%**	1
Bulgaria	**2**	**4**	**0.0%**	-	**100.0%**	2	**0.0%**	-	**0.0%**	-
Canada	**21**	**25**	**0.0%**	-	**71.4%**	15	**9.5%**	2	**19.0%**	4
Chile	**1**	**1**	**0.0%**	-	**0.0%**	-	**0.0%**	-	**100.0%**	1
China	**3**	**42**	**0.0%**	-	**100.0%**	3	**0.0%**	-	**0.0%**	-
Colombia	**2**	**3**	**0.0%**	-	**50.0%**	1	**0.0%**	-	**50.0%**	1
Czech Republic	**13**	**29**	**0.0%**	-	**53.8%**	7	**15.4%**	2	**30.8%**	4
Denmark	**16**	**106**	**0.0%**	-	**75.0%**	12	**18.8%**	3	**6.3%**	1
Estonia	**2**	**5**	**0.0%**	-	**100.0%**	2	**0.0%**	-	**0.0%**	-
Finland	**11**	**22**	**0.0%**	-	**100.0%**	11	**0.0%**	-	**0.0%**	-
France	**338**	**645**	**0.0%**	-	**76.3%**	258	**14.5%**	49	**9.2%**	31
French Polynesia	**1**	**1**	**0.0%**	-	**100.0%**	1	**0.0%**	-	**0.0%**	-
French Southern Territories	**1**	**1**	**0.0%**	-	**0.0%**	-	**100.0%**	1	**0.0%**	-
Germany	**558**	**2,309**	**0.0%**	-	**86.4%**	482	**8.6%**	48	**5.0%**	28
Greece	**6**	**59**	**0.0%**	-	**83.3%**	5	**16.7%**	1	**0.0%**	-
Hong Kong	**1**	**1**	**0.0%**	-	**0.0%**	-	**100.0%**	1	**0.0%**	-
Hungary	**2**	**3**	**0.0%**	-	**100.0%**	2	**0.0%**	-	**0.0%**	-
Iceland	**2**	**3**	**0.0%**	-	**50.0%**	1	**50.0%**	1	**0.0%**	-
India	**43**	**102**	**0.0%**	-	**79.1%**	34	**2.3%**	1	**18.6%**	8
Ireland	**4**	**4**	**0.0%**	-	**0.0%**	-	**0.0%**	-	**100.0%**	4
Israel	**11**	**34**	**0.0%**	-	**45.5%**	5	**0.0%**	-	**54.5%**	6
Italy	**79**	**153**	**0.0%**	-	**57.0%**	45	**11.4%**	9	**31.6%**	25
Japan	**25**	**67**	**0.0%**	-	**96.0%**	24	**4.0%**	1	**0.0%**	-
Korea Republic Of	**13**	**19**	**0.0%**	-	**84.6%**	11	**0.0%**	-	**15.4%**	2
Latvia	**1**	**1**	**0.0%**	-	**100.0%**	1	**0.0%**	-	**0.0%**	-
Lithuania	**6**	**20**	**0.0%**	-	**50.0%**	3	**16.7%**	1	**33.3%**	2
Luxembourg	**33**	**90**	**0.0%**	-	**75.8%**	25	**24.2%**	8	**0.0%**	-
Malta	**3**	**8**	**0.0%**	-	**66.7%**	2	**33.3%**	1	**0.0%**	-
Mexico	**1**	**3**	**0.0%**	-	**100.0%**	1	**0.0%**	-	**0.0%**	-
Monaco	**2**	**2**	**0.0%**	-	**50.0%**	1	**0.0%**	-	**50.0%**	1
Norway	**13**	**27**	**0.0%**	-	**69.2%**	9	**30.8%**	4	**0.0%**	-
Poland	**13**	**14**	**0.0%**	-	**84.6%**	11	**7.7%**	1	**7.7%**	1
Qatar	**1**	**1**	**0.0%**	-	**100.0%**	1	**0.0%**	-	**0.0%**	-
Russian Federation	**3**	**6**	**0.0%**	-	**100.0%**	3	**0.0%**	-	**0.0%**	-
Singapore	**1**	**2**	**0.0%**	-	**100.0%**	1	**0.0%**	-	**0.0%**	-
Slovakia	**1**	**1**	**0.0%**	-	**0.0%**	-	**0.0%**	-	**100.0%**	1
Spain	**9**	**135**	**0.0%**	-	**77.8%**	7	**0.0%**	-	**22.2%**	2
Sweden	**74**	**400**	**0.0%**	-	**89.2%**	66	**2.7%**	2	**8.1%**	6
Switzerland	**43**	**80**	**0.0%**	-	**62.8%**	27	**25.6%**	11	**11.6%**	5
Taiwan Province Of China	**155**	**619**	**0.0%**	-	**98.1%**	152	**0.6%**	1	**1.3%**	2
Turkey	**2**	**8**	**0.0%**	-	**100.0%**	2	**0.0%**	-	**0.0%**	-
Ukraine	**5**	**32**	**0.0%**	-	**80.0%**	4	**20.0%**	1	**0.0%**	-
United Kingdom	**759**	**1,564**	**0.0%**	-	**86.3%**	655	**9.7%**	74	**4.0%**	30
United States	**978**	**3,507**	**0.0%**	-	**80.8%**	790	**11.2%**	110	**8.0%**	78

Microsoft

Data Glossary of Terms

Total Number of Law Enforcement Requests
The number of criminal requests received from a law enforcement agency and/or court seeking customer data. Examples of the types of requests include a subpoena, a court order, and a warrant.

Accounts/Users Specified
The total number of usernames, accounts, or other identifiers that were specified in the requests received. One law enforcement request could include the names of multiple users, and/or could include multiple accounts associated with a single user. For example, one user could have multiple accounts – such as an Outlook.com E-mail account, an Xbox Gamertag, a Microsoft Account ID, or an Xbox serial number.

Law Enforcement Requests Resulting in Disclosure of Content
The number of court orders found to be lawful, and therefore at least some customer content was disclosed. Such content could include the subject or body of an email, photos stored in SkyDrive, address book information, and calendars. In most cases, a court order that requires the disclosure of customer content will also require the disclosure of non-content data (see definition below).

Law Enforcement Requests Resulting in Disclosure of Only Subscriber/Transactional (Non-Content) Data
The number of law enforcement requests determined to be lawful, and therefore only non-content information was disclosed. Non-content information could include the user's name, billing address, IP history, etc.

Law Enforcement Requests Resulting in Disclosure of No Customer Data (Request Rejected for Not Meeting Legal Requirements)
The number of law enforcement requests and/or court orders rejected because we determined they failed to satisfy the relevant legal requirements, or where we successfully redirected law enforcement to obtain the information directly from the customer. As a result, no customer data of any kind was disclosed.

Law Enforcement Requests Resulting in Disclosure of No Customer Data (No Data Found)
The number of law enforcement requests and/or court orders where our Compliance Team found no data in our systems related to the request and/or order, and therefore disclosed no customer information to law enforcement.

Percentage
All percentages are calculated by dividing the associated column by the Total Number of Requests.

Microsoft

2013 Microsoft Law Enforcement Requests Report
Frequently Asked Questions

How many Microsoft and Skype users were impacted by law enforcement requests?

It is difficult to determine how many individual customers are potentially impacted by law enforcement requests because a single request may include multiple accounts for one user or multiple accounts for many individuals or it may not affect any customers because the account identifier is invalid. In the context of Skype, because law enforcement sometimes submits requests seeking to identify which users placed phone calls – based on the number called and the date, time and duration of the call – the number of users impacted by the requests is, in that context, lower than the number of identifiers included in the law enforcement request.

For the first six months of 2013, the law enforcement requests Microsoft received requested information about 66,539 Microsoft and Skype accounts or identifiers. We have many hundreds of millions of accounts across our online and cloud services. To give you a sense of proportion, we estimate that fewer than one one-hundredth of one percent (0.01%) of Microsoft or Skype accounts were potentially affected by law enforcement requests during this period.

In the context of our enterprise services, in the first half of 2013, we addressed a total of 19 requests for e-mail accounts we host for entities, such as universities or other businesses. Those 19 requests sought information about 48 accounts. We disclosed customer data in response to five of those requests (4 content; 1 only non-content), and in all but one case, we were able to notify the customer. We rejected the request, found no responsive data, or redirected law enforcement to obtain the information from the customer directly in 13 of those cases. One request is still pending. The data show that law enforcement sought information about only a tiny fraction of the millions of end users of our enterprise services, such as Office 365. In all 19 cases, the legal demands were from law enforcement entities located in the U.S., and sought data about accounts associated with enterprise customers located in the United States. In addition, to date, Microsoft has not disclosed enterprise customer data in response to a government request issued pursuant to national security laws.

How many times did Microsoft disclose the content of customer communications or data storage to law enforcement?

In the first half of 2013, Microsoft disclosed content in response to 2.2% of the total number of law enforcement requests received. Each of those disclosures was in response to a court order or warrant, and the vast majority of those disclosures related to users of our consumer services.

Are Microsoft and Skype data reported separately?

When we published our first report in March 2013, we reported Microsoft and Skype data separately, but noted that we were aligning our reporting formats across all Microsoft services so it could be presented in the same manner. Because the reporting formats have now been aligned, we are publishing a single report that includes data on the number of law enforcement requests for all Microsoft services, including Skype. Because this is the first time we will be publishing a report that merges Skype with the rest of Microsoft's services, we have decided to include an additional report that separates out the law enforcement requests for information about Skype users.

Microsoft received requests from more foreign governments, and received them in greater volume, than some other companies. Why?

Microsoft maintains operations and a physical presence in more than 100 countries around the world, as a result of which law enforcement authorities and/or courts may contact local Microsoft offices with requests for customer data. However, we only disclose data to law enforcement after validating the lawfulness of the request.

What services are subject to law enforcement requests?

As our law enforcement request reports have shown, the overwhelming majority of law enforcement requests seek information related to our free consumer services used by individuals in their personal capacity such as: web-mail accounts (Hotmail/Outlook.com), SkyDrive cloud storage; Messenger, and Skype. We also receive requests related to Xbox Live users. In all instances, unless an individual subscribes to a paid-for service, such as Xbox Live, Microsoft cannot and does not verify an individual's identity. By comparison, we have received comparatively few law enforcement requests for data associated with our enterprise customers. Our law enforcement request data reflects only 19 requests for enterprise customer data, concerning e-mail accounts we host and administer for other businesses or institutions.

What is the difference between a consumer service and an enterprise service?

A consumer service is generally one subscribed to and used by an individual in his or her personal capacity. Some examples include Hotmail/Outlook.com, SkyDrive, Xbox Live and Skype. An enterprise service is generally subscribed to by an entity ranging from a small business to large multi-national corporations, institutions and governmental entities. Those entities, in-turn, may provide services, such as e-mail, to individual employees, students or others. Some enterprise cloud offerings include Office 365, Azure and Exchange Online and CRM Online.

What is non-content data?

Non-content data refers to basic subscriber information, such as the e-mail address, name, location and IP address captured at the time of registration. Below is an example of exactly what law enforcement receives when Microsoft produces basic subscriber information, using a test account registered by a Microsoft employee. Although we changed the name and are masking the extension for security reasons, all other information is exactly what Microsoft produces to law enforcement.

Field	Value
Login	First.Last@xxxxxxx.com
PUID	0006BFFDA0FF8810
First Name	First
Last Name	Last
State	Washington
Zip	98052
Country	US
Timezone	America/Los_Angeles
Registered from IP	65.55.161.10
Date Registered {Pacific}	10/24/2007 1:05:18 PM
Gender	M

Last Login IP	64.4.1.11

The PUID in the above table stands for "Personal User ID," which is a unique alpha-numeric code generated for each registered Microsoft account. Other non-content data may include IP connection history, an Xbox Gamertag, and credit card or other billing information. We require an official, document based request, such as a subpoena, before we will consider disclosing non-content data to law enforcement.

What is content data?

Content is what our customers create, communicate, and store on or through our services such as the words in an e-mail exchanged between friends or business colleagues or the photographs and documents stored on SkyDrive or in other cloud offerings such as Office 365 and Azure. We require a court order or warrant before we will consider disclosing content to law enforcement.

What should Microsoft and Skype customers take away from this data disclosure?

Microsoft's mission is to help people and businesses across the globe realize their full potential, and all of our technologies are designed to further that mission. We place a premium on respecting and protecting the privacy of our users, and work to earn their trust every day. At the same time, Microsoft recognizes that law enforcement plays a critically important role in keeping our users – and our technology – safe and free from abuse or exploitation. We are hopeful that this data disclosure can better inform all sides in the critically important public discussion about how best to strike the balance between the privacy of our customers and the legitimate needs of law enforcement agencies that protect and serve their citizens.

Did Microsoft ever challenge a law enforcement request?

As our report shows, a number of law enforcement requests were rejected across all Microsoft services (2.5%), including Skype (7.3%). Challenges to government requests can take many forms. In many of these cases, we simply inform the requesting government that we are unable to disclose the requested information, and explain our reason for doing so. We also consider whether it is appropriate to challenge a particular request in court.

Does the data include any legal demands that may have been issued pursuant to U.S. national security orders (e.g. FISA Orders and FISA Directives)?

To date, we have gone as far as we are legally permitted in disclosing information about government demands for customer data, but we would like to go further. The number of requests included in this report only include requests from law enforcement entities. It does not, however, include any requests that may have been issued pursuant to national security authorities, such as the Foreign Intelligence Surveillance Act (FISA) in the United States. In June, we published aggregate data, covering the six-month period of July 1, 2012 thru December 31, 2012, that included any U.S. national security orders Microsoft and/or Skype may have received (including, if any, FISA Orders and FISA Directives). As we noted then, only a tiny fraction of our users were impacted by U.S. Government requests. We have also tried to provide additional information about our process for handling government requests for customer data.

We believe it is important to provide additional detail about the various types of requests we receive, and we look forward to publishing a comprehensive report that includes detailed information about all types of government demands we may receive for user data, including any requests pursuant to national security authorities, when we are legally permitted to do that. To that end, we have filed a lawsuit in the Foreign Intelligence Surveillance Court (FISC) requesting permission to disclose detailed information about any national security orders that we may have received. **We have published some information about National Security Letters that we have received (see below).**

Did Microsoft or Skype receive any National Security Letters (NSLs)?

Pursuant to approval from the government, we are able to provide, on an annual basis, the following information about National Security Letters (NSLs) served on Microsoft. Information about any NSLs we may receive during 2013 would be included in the next version of this report. The Director of the Federal Bureau of Investigation (FBI) and other senior FBI officials are authorized to issue National Security Letters to electronic communication service providers, such as Microsoft, to obtain "the name, address, length of service, and local and long distance toll billing records" of our users if it is "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities."

Period	Number of NSLs	Identifiers	NSLs Seeking Content	Identifiers	NSLs Seeking Only Non-content	Identifiers

2012	0-999	1,000 – 1,999	N/A	N/A	0-999	1,000 – 1,999
2011	1,000 – 1,999	3,000 – 3,999	N/A	N/A	1,000 – 1,999	3,000 – 3,999
2010	1,000 – 1,999	5,000 – 5,999	N/A	N/A	1,000 – 1,999	5,000 – 5,999
2009	0 – 999	2,000 – 2,999	N/A	N/A	0 – 999	2,000 – 2,999

Does Microsoft have a program to disclose information in response to imminent emergencies?

Yes, consistent with industry practice and as permitted by law, we do, in limited circumstances, disclose information to criminal law enforcement agencies where we believe the disclosure is necessary to prevent an emergency involving danger of death or serious physical injury to a person. Microsoft considers emergency requests from law enforcement agencies around the world. Those requests must be in writing on official letterhead, and signed by a law enforcement authority. The request must contain a summary of the emergency, along with an explanation of how the information sought will assist law enforcement in addressing the emergency. Each request is carefully evaluated by Microsoft's compliance team before any data is disclosed, and the disclosure is limited to the data that we believe would enable law enforcement to address the emergency. Some of the most common emergency requests involve suicide threats and kidnappings. A summary of the emergency requests received in the first half of 2013 is below.

Country	Total Number of Requests	Accounts/Users Specified in Requests	Some Customer Data Disclosed				No Customer Data Disclosed			
			Requests Resulting in Disclosure of Content		Requests Resulting in Disclosure of Only Subscriber/Transactional (Non-Content) Data		Requests Resulting in Disclosure of No Customer Data (No Data Found)		Requests Resulting in Disclosure of No Customer Data(Request Rejected for Not Meeting Legal Requirements)	
			%	#	%	#	%	#	%	#
TOTAL	**346**	**487**	**32.4%**	**112**	**39.0%**	**135**	**17.3%**	**60**	**11.3%**	**39**
Argentina	2	2	**100.0%**	2	**0.0%**	-	**0.0%**	-	**0.0%**	-
Belgium	4	4	**0.0%**	-	**75.0%**	3	**25.0%**	1	**0.0%**	-
Canada	23	27	**13.0%**	3	**52.2%**	12	**8.7%**	2	**26.1%**	6
Colombia	1	1	**100.0%**	1	**0.0%**	-	**0.0%**	-	**0.0%**	-

Denmark	2	2	**0.0%**	-	**0.0%**	-	**100.0%**	2	**0.0%**	-
Finland	1	1	**0.0%**	-	**100.0%**	1	**0.0%**	-	**0.0%**	-
France	29	49	**27.6%**	8	**41.4%**	12	**27.6%**	8	**3.4%**	1
Germany	37	50	**75.7%**	28	**2.7%**	1	**21.6%**	8	**0.0%**	-
Ireland	1	2	**0.0%**	-	**0.0%**	-	**100.0%**	1	**0.0%**	-
Italy	2	2	**0.0%**	-	**100.0%**	2	**0.0%**	-	**0.0%**	-
Mexico	62	100	**64.5%**	40	**6.5%**	4	**14.5%**	9	**14.5%**	9
Netherlands	1	1	**0.0%**	-	**0.0%**	-	**100.0%**	1	**0.0%**	-
Norway	2	2	**50.0%**	1	**0.0%**	-	**50.0%**	1	**0.0%**	-
Poland	2	2	**0.0%**	-	**0.0%**	-	**100.0%**	2	**0.0%**	-
Portugal	1	1	**0.0%**	-	**100.0%**	1	**0.0%**	-	**0.0%**	-
Spain	9	19	**55.6%**	5	**33.3%**	3	**11.1%**	1	**0.0%**	-
Sweden	1	1	**0.0%**	-	**100.0%**	1	**0.0%**	-	**0.0%**	-
Switzerland	1	1	**100.0%**	1	**0.0%**	-	**0.0%**	-	**0.0%**	-
Turkey	1	1	**0.0%**	-	**0.0%**	-	**0.0%**	-	**100.0%**	1
United Kingdom	77	89	**7.8%**	6	**64.9%**	50	**19.5%**	15	**7.8%**	6
United States	87	130	**19.5%**	17	**51.7%**	45	**10.3%**	9	**18.4%**	16

Microsoft

Principles, Policies and Practices
Frequently Asked Questions

What are Microsoft and Skype's principles and policies in respect to law enforcement requests?

Microsoft and Skype require law enforcement entities to follow the laws, rules and procedures for requesting customer data in criminal investigations. We require a valid subpoena or equivalent document before we will consider releasing non-content data; and we require a court order or warrant before we will consider producing content.

What is the process for disclosing customer information to law enforcement?

Both Microsoft and Skype require an official, signed document, issued pursuant to local law and rules to be delivered to our compliance teams based in the U.S. and Ireland for Microsoft data and Luxembourg for Skype.

For law enforcement requests for Microsoft customer data from non-English speaking countries, a local team or individual, typically a lawyer or someone operating under legal guidance will receive and authenticate the law enforcement request. If it complies with local law, then it will be translated and sent to the Microsoft compliance teams in the U.S. or Ireland. Skype's compliance team members speak multiple languages and assess the validity of most requests, especially those from European law enforcement entities, sent directly to the team in Luxembourg, which is the same procedure Skype employed prior to the Microsoft acquisition.

What laws apply to Microsoft and Skype customer records and content?

For data hosted in the U.S., Microsoft follows the Electronic Communications Privacy Act. We require at least a subpoena before turning over non-content records, such as basic subscriber information or IP connection history and we require an order or warrant before producing content. Irish law and European Union directives apply to the Hotmail and Outlook.com accounts hosted in Ireland. Skype is a wholly-owned, but independent division of Microsoft, headquartered in and operating pursuant to Luxembourg law.

How does Microsoft and Skype determine what law enforcement entities are able to request data?

Microsoft must produce data in response to valid legal requests from U.S. and Irish law enforcement entities because we are headquartered in those jurisdictions or because we host data in those countries. Microsoft may disclose non-content data pursuant to a law enforcement request after it is validated locally and transmitted to our compliance teams in the U.S. and Ireland. Skype must produce data to Luxembourg authorities and is able to disclose some records to law enforcement entities outside of Luxembourg.

What is Microsoft and Skype's position on CALEA?

The U.S. law, Communications Assistance for Law Enforcement Act, does not apply to any of Microsoft's services, including Skype, as Microsoft is not a telecommunications carrier. Skype is an independent division headquartered and operating under Luxembourg law.

Why do Microsoft and/or Skype reject a law enforcement request?

There are a number of reasons why Microsoft or Skype may reject a law enforcement request. For example we may reject it if it is not signed or appropriately authorized, contains the wrong dates, is not properly addressed, contains material mistakes or if it is overly broad.

If a request was rejected, can you assure your customer that their information was not disclosed?

No. While no customer information is provided to law enforcement in response to a rejected request, it is possible that law enforcement later submit a valid request for the same information.

Does Microsoft reject subpoenas from law enforcement seeking content data?

Yes. We require an order or warrant before we will consider releasing content. Like other companies, we implemented the holding of U.S. v. Warshak, which held a provision of the Electronic Communications Privacy Act to be unconstitutional.

How does Microsoft consider potential human rights issues impacted by law enforcement requests?

Our Global Human Rights Statement outlines our commitment to respect the human rights of our customers. By verifying law enforcement entities followed the laws and procedures in their jurisdictions before we respond to a request, we seek to ensure we are disclosing customer data in

authorized criminal investigations. We respect the fact that law enforcement entities have the very difficult job of keeping us all safe and bringing to justice those who commit crimes. At the same time, we remain cognizant of the potential for law enforcement activities to infringe upon human rights and free expression.

Does Microsoft provide anything to law enforcement absent a legal request?

Occasionally. Pursuant to United States law, we are required to report identified or suspected images exploiting children to the United States' National Center for Missing and Exploited Children (NCMEC). We also, on occasion, report some limited information about a user when we have reason to believe the individual is about to harm themselves or someone else due to a public posting on one of our forums, on Xbox LIVE, or through referrals from other customers. If one of our customers or employees, or Microsoft itself, is the victim of a crime, we may report some limited information to law enforcement. Additionally, consistent with applicable law and industry practice, Microsoft sometimes discloses limited information where we believe the disclosure is necessary to prevent an emergency involving danger of death or serious physical injury to a person. Microsoft considers emergency requests from law enforcement agencies around the world. Those requests must be in writing on official letterhead, and signed by a law enforcement authority. The request must contain a summary of the emergency, along with an explanation of how the information sought will assist law enforcement in addressing the emergency. Each request is carefully evaluated by Microsoft's compliance team before any data is disclosed, and the disclosure is limited to the data that we believe would enable law enforcement to address the emergency.

Does Microsoft charge law enforcement for providing data and content?

Yes. Pursuant to the Electronic Communications Privacy Act, Microsoft is entitled to seek reimbursement for costs associated with compliance with a valid U.S. law enforcement request. We only charge U.S. law enforcement entities pursuant to industry rates and only in an attempt to recover some costs associated with the need to comply with U.S. legal demands. We do not, however, charge in emergency situations or in known child exploitation investigations.