

# Law Enforcement Requests Report 2012

**March 21, 2013**

# Law Enforcement Requests Report 2012

Requests received for Microsoft Services (excluding Skype) from Jan – Dec, 2012

	Total Requests		Some Customer Data Disclosed				No Customer Data Disclosed			
	Total Number of Law Enforcement Requests	Accounts / Users Specified in Requests	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 (Request Rejected for Not Meeting Legal Requirements)		Law Enforcement Requests Resulting in Disclosure of No Customer Data (No Data Found)	
			#	#	%	#	%	#	%	#
<b>TOTAL</b>	<b>70,665</b>	<b>122,015</b>	<b>2.2%</b>	<b>1,558</b>	<b>79.8%</b>	<b>56,388</b>	<b>1.2%</b>	<b>866</b>	<b>16.8%</b>	<b>11,852</b>
Argentina	769	1,279	0.0%	-	85.7%	659	0.0%	-	14.3%	110
Australia	2,238	3,081	0.0%	-	84.9%	1,899	1.0%	23	14.1%	316
Belgium	727	1,140	0.0%	-	86.5%	629	0.0%	-	13.5%	98
Brazil	2,214	4,176	0.3%	7	84.1%	1,862	0.1%	2	15.5%	343
Canada	103	385	1.0%	1	93.2%	96	1.0%	1	4.9%	5
Chile	530	791	0.0%	-	84.3%	447	0.0%	-	15.7%	83
Colombia	227	623	0.0%	-	83.3%	189	0.0%	-	16.7%	38
Costa Rica	98	152	0.0%	-	92.9%	91	0.0%	-	7.1%	7
Czech Republic	19	27	0.0%	-	84.2%	16	0.0%	-	15.8%	3
Denmark	128	191	0.0%	-	86.7%	111	0.0%	-	13.3%	17
Dominican Republic	17	228	0.0%	-	100.0%	17	0.0%	-	0.0%	-
Ecuador	59	95	0.0%	-	96.6%	57	0.0%	-	3.4%	2
El Salvador	9	10	0.0%	-	88.9%	8	0.0%	-	11.1%	1
Finland	56	328	0.0%	-	96.4%	54	0.0%	-	3.6%	2
France	8,603	17,973	0.0%	-	85.7%	7,377	0.0%	4	14.2%	1,221
Germany	8,419	13,226	0.0%	-	84.2%	7,088	0.1%	5	15.8%	1,326
Greece	9	11	0.0%	-	66.7%	6	0.0%	-	33.3%	3
Guatemala	2	4	0.0%	-	100.0%	2	0.0%	-	0.0%	-
Hong Kong	1,041	1,049	0.0%	-	79.0%	822	0.3%	3	20.7%	216
Hungary	123	175	0.0%	-	82.9%	102	0.0%	-	17.1%	21
Iceland	8	9	0.0%	-	87.5%	7	0.0%	-	12.5%	1
India	418	594	0.0%	-	88.5%	370	1.0%	4	10.5%	44
Ireland	72	222	6.9%	5	63.9%	46	2.8%	2	26.4%	19
Israel	54	141	0.0%	-	85.2%	46	0.0%	-	14.8%	8
Italy	1,519	2,098	0.0%	-	83.0%	1,261	0.0%	-	17.0%	258
Japan	572	766	0.0%	-	94.1%	538	0.5%	3	5.4%	31
Korea	616	1,091	0.0%	-	81.3%	501	0.0%	-	18.7%	115
Luxembourg	55	81	0.0%	-	87.3%	48	0.0%	-	12.7%	7
Malta	75	79	0.0%	-	89.3%	67	0.0%	-	10.7%	8
Mexico	1,323	2,979	0.0%	-	90.2%	1,194	0.0%	-	9.8%	129
Netherlands	859	1,438	0.0%	-	78.1%	671	0.1%	1	21.8%	187
New Zealand	64	128	1.6%	1	71.9%	46	3.1%	2	23.4%	15
Norway	187	426	0.0%	-	89.8%	168	0.5%	1	9.6%	18
Panama	26	32	0.0%	-	92.3%	24	0.0%	-	7.7%	2
Peru	84	257	0.0%	-	92.9%	78	0.0%	-	7.1%	6
Poland	70	110	0.0%	-	78.6%	55	0.0%	-	21.4%	15
Portugal	548	710	0.0%	-	85.6%	469	0.2%	1	14.2%	78
Singapore	179	553	0.0%	-	93.9%	168	0.0%	-	6.1%	11
Slovakia	28	29	0.0%	-	89.3%	25	0.0%	-	10.7%	3
Slovenia	1	1	0.0%	-	0.0%	-	0.0%	-	100.0%	1
Spain	1,981	3,400	0.0%	-	84.2%	1,668	0.1%	1	15.7%	312
Sweden	326	552	0.0%	-	89.9%	293	0.0%	-	10.1%	33
Taiwan	4,381	8,305	0.0%	-	86.3%	3,779	0.0%	-	13.7%	602
Thailand	83	105	0.0%	-	88.0%	73	0.0%	-	12.0%	10
Turkey	11,434	14,077	0.0%	-	78.7%	8,997	0.0%	4	21.3%	2,433
United Kingdom	9,226	14,301	0.0%	-	76.5%	7,057	0.5%	50	23.0%	2,119
United States	11,073	24,565	13.9%	1,544	65.0%	7,196	6.9%	759	14.2%	1,574
Uruguay	1	1	0.0%	-	100.0%	1	0.0%	-	0.0%	-
Venezuela	11	21	0.0%	-	90.9%	10	0.0%	-	9.1%	1

# Law Enforcement Requests Report 2012

Requests received for Skype from Jan – Dec, 2012

	Calendar Year 2012			July 2012 - December 2012	
	Total Number of Law Enforcement Requests	Accounts / Identifiers Specified in Requests	Requests Resulting in Disclosure of Content	Accounts Specified Where Compliance Team Found No Data	Provided Guidance to Law Enforcement
<b>TOTAL</b>	<b>4,713</b>	<b>15,409</b>		<b>2,847</b>	<b>501</b>
Argentina	2	5	0	1	1
Armenia	2	6	0	3	-
Australia	195	424	0	118	8
Austria	10	18	0	-	4
Belarus	5	35	0	-	-
Belgium	39	165	0	45	3
Brazil	8	36	0	1	-
Bulgaria	7	15	0	6	2
Canada	20	58	0	5	12
China	6	50	0	2	-
Czech Republic	33	109	0	23	1
Denmark	16	41	0	9	5
Estonia	6	12	0	2	-
Finland	7	9	0	2	-
France	402	827	0	110	27
Germany	686	2,646	0	475	70
Greece	9	11	0	3	-
Hong Kong	-	-	0	-	3
Hungary	7	28	0	2	-
Iceland	2	4	0	1	1
India	53	101	0	47	10
Ireland	4	7	0	-	2
Israel	10	14	0	-	-
Italy	96	648	0	171	17
Japan	40	88	0	17	45
Korea	7	9	0	-	3
Latvia	5	60	0	-	-
Lebanon	1	1	0	-	-
Lithuania	8	35	0	2	-
Luxembourg	98	446	0	-	3
Malta	5	9	0	5	-
Mexico	3	10	0	2	-
Netherlands	2	2	0	-	-
New Zealand	1	2	0	-	1
Norfolk Island	-	-	0	-	1
Norway	14	23	0	-	2
Pakistan	-	-	0	-	2
Poland	17	42	0	18	5
Portugal	1	1	0	-	-
Puerto Rico	2	4	0	-	-
Qatar	2	5	0	-	-
Russian Federation	2	5	0	1	-
Singapore	4	5	0	1	-
Slovakia	1	1	0	-	-
Slovenia	1	3	0	2	-
South Africa	1	6	0	-	-
South Georgia	-	-	0	-	1
Spain	11	40	0	2	4
Sweden	43	150	0	5	4
Switzerland	74	148	0	42	10
Taiwan	316	1,499	0	247	3
Tanzania	1	1	0	-	-
Ukraine	5	10	0	1	-
United Arab Emirates	1	1	0	-	1
United Kingdom	1,268	2,720	0	444	40
United States	1,154	4,814	0	1,032	210

# Law Enforcement Requests Report 2012

## Glossary of Terms

### **Total Number of 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 Microsoft found to be lawful, and therefore disclosed at least some customer content. 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 information (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.

### **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 Microsoft rejected because we determined they failed to satisfy the relevant legal requirements. As a result, no data of any kind was disclosed.

### **Requests Resulting in Disclosure of No Customer Data (No Data Found)**

The number of law enforcement requests and/or court orders where the Microsoft 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.

### **Accounts Specified in Requests Where Compliance Team Found No Data**

The number of times the Skype compliance team searched for a username or other identifier (e.g., PSTN number) specified in a valid law enforcement request but found no data.

### **Provided Guidance to Law Enforcement**

The number of times the Skype compliance team provided general guidance to a domestic or foreign law enforcement agency, either in response to a rejected request or general questions, about the process for obtaining Skype user data.

# Law Enforcement Requests Report 2012

## What the Data Shows

*Microsoft Releases 2012 Law Enforcement Report by Brad Smith, General Counsel and Executive Vice President, Legal and Corporate Affairs, Microsoft.*

This is our first Law Enforcement Requests Report. It provides data on the number of requests we received from law enforcement agencies around the world relating to Microsoft online and cloud services and how we responded to those requests. All of our major online services are covered in this report, including, for example, Hotmail, Outlook.com, SkyDrive, Xbox LIVE, Microsoft Account, and Office 365. We're also making available similar data relating to Skype, which Microsoft acquired in October 2011.

We will update this report every six months.

### Our Perspective

In recent months, there has been broadening public interest in how often law enforcement agencies request customer data from technology companies and how our industry responds to these requests. Google, Twitter and others have made important and helpful contributions to this discussion by publishing some of their data. We've benefited from the opportunity to learn from them and their experience, and we seek to build further on the industry's commitment to transparency by releasing our own data today.

Like others in the industry, we are releasing publicly the total number of requests we receive from law enforcement in countries around the world and the number of potentially affected accounts identified in those requests.

We are also publishing additional data that we hope will provide added insights for our customers and the public who are interested in these issues. For example, we are providing more detailed information that shows the number of law enforcement requests resulting in disclosure to these agencies of "customer content", such as the subject line and body of an email exchanged through Outlook.com; or a picture stored on SkyDrive. We similarly are reporting on the number of law enforcement requests that result in

disclosure only of "non-content" data, which includes account information such as an email address, a person's name, country of residence, or gender, or system-generated data such as IP addresses and traffic data.

As most people recall, Microsoft acquired Skype toward the end of 2011, and the integration of our two companies advanced considerably over the course of 2012. Not surprisingly, Skype collected and retained certain data in different formats than the rest of Microsoft. It is therefore presented differently in this first report, which covers last year. Going forward, we are aligning our reporting formats across all Microsoft services, including Skype, so they can be presented in the same manner in our future reports. We also will continue to look for new ways to improve the usefulness of the data we publish, and I know we'll benefit from the feedback that we'll continue to receive from individuals and groups around the world.

### What the Data Shows

A lot of the public discussion about law enforcement requests to tech companies has focused on the benefits of transparency. While transparency is definitely valuable, it's also important to step back when reports like this are released and ask what the data actually shows. We've made the data available in a format that enables anyone to analyze it (and as I've found, the new PowerPivot feature in Excel is so easy that even a lawyer can make ready use of it). As I've had the opportunity in recent weeks to review all of our data and talk with the Microsoft teams that work in this area, a few themes have struck me as the most significant. I've therefore tried to summarize below what has struck me as some of the principal trends reflected in the data we're releasing today:

- First, while we receive a significant number of law enforcement requests from around the world, very few actually result in the disclosure to these agencies of customer content. To be precise, last year Microsoft (including Skype) received 75,378 law enforcement requests for customer information, and these requests potentially affected 137,424 accounts or other identifiers. **Only 2.1 percent, or 1,558 requests, resulted in the disclosure of customer content.**
- It's insightful, I believe, to look at the governments to whom customer content was disclosed. **Of the 1,558 disclosures of customer content, more than 99 percent were in response to lawful warrants from courts in the United States.** In fact, there were only 14 disclosures of

# Law Enforcement Requests Report 2012

customer *content* to governments outside the United States. These were to governments in Brazil, Ireland, Canada and New Zealand.

- Of the 56,388 cases where Microsoft (excluding Skype) disclosed some non-content information to law enforcement agencies, **more than 66 percent of these were to agencies in only five countries**. These were the U.S., the United Kingdom, Turkey, Germany and France. For Skype, the top five countries accounted for 81 percent of all requests. These countries were the U.K., U.S., Germany, France and Taiwan.
- **Roughly 18 percent of the law enforcement requests (again, excluding Skype) resulted in the disclosure of no customer information in any form**, either because Microsoft rejected the request or because no customer information was found. (We don't have this information for Skype for 2012 because its data was not retained in this form, but we will for 2013 and the future.)
- We addressed last year a total of **only 11 law enforcement requests for information relating to Microsoft's enterprise customers**. In general, we believe that law enforcement requests for information from an enterprise customer are best directed to that customer rather than a tech company that happens to host that customer's data. That way, the customer's legal department can engage directly with law enforcement personnel to address the issue. Last year, we either rejected or were successful in redirecting seven of these 11 requests, and in the four instances where we disclosed some enterprise customer information, we either obtained the customer's consent before complying, or we disclosed the information pursuant to a specific contractual arrangement to process such requests on behalf of the customer. (For more on how Microsoft handles requests for enterprise customer information, please visit our [FAQ](#))
- Finally, while law enforcement requests for information unquestionably are important (and raise important issues around the world), only a tiny percentage of users are potentially affected by them. We have many hundreds of millions of accounts across our online and cloud services. **To give you a sense of proportion, we estimate that less than two one-hundredths of one percent (or 0.02 percent, to put it another way) were potentially affected by law enforcement requests**. This broke down as follows:

- Microsoft services (excluding Skype) received 70,665 requests from law enforcement, impacting a potential 122,015 accounts or other identifiers.

- Skype received 4,713 requests from law enforcement. Those requests impacted 15,409 accounts or other identifiers, such as a PSTN number. **Skype produced no content in response to these requests**, but did provide *non-content data*, such as a SkypeID, name, email account, billing information and call detail records if a user subscribed to the Skype In/Online service, which connects to a telephone number.

## What We Do

As we continue to move forward, Microsoft is 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. Like every company, we are obligated to comply with legally binding requests from law enforcement, and we respect and appreciate the role that law enforcement personnel play in so many countries to protect the public's safety.

While these issues are sometimes complex, we strive to follow practices that are clear and straightforward:

- We require a valid subpoena or legal equivalent before we will consider releasing a customer's non-content data to a law enforcement agency.
- We require a court order or warrant before we will consider releasing a customer's content to law enforcement.
- We take a close look in each instance to ensure that the requests we receive for a customer's information are in accord with the laws, rules and procedures that are applicable to requests for customer data and content.
- You can find additional detailed information on our policies and practices in our [FAQ](#).

## Looking Forward

This is obviously our first report of this nature. We welcome suggestions and feedback, and we'll no doubt continue to learn from our own experience as well as from others as we move forward. If you have ideas you'd like us to consider, please send them to us by email to [mciti\\_zen@microsoft.com](mailto:mciti_zen@microsoft.com). Even though we may not ultimately agree with or adopt every suggestion, I know we'll be better off for having received and considered your ideas.

Thanks.