CyberGhost Transparency Report 2015

CyberGhost is no one's Honeypot!

Founded 2011 in Bucharest, Romania, CyberGhost is the creator of one of the world's most reliable privacy and security solutions in the world. The company secures and anonymizes the online presence of over 7.5 million users across the globe. CyberGhost defends privacy as a basic human right, being first in the industry to publish a transparency report while building new user-oriented crypto-technology for the future.

The transparency report aims to highlight insights of various requests to disclose the identity of CyberGhost's users. The requests received by law enforcement agencies, police offices, and websites owners or individuals and law firms around the world have been grouped in three categories: DMCA complaints, police requests and malware activity complaints.

CyberGhost considers privacy a basic human right as well as the foundation of democratic societies. Even though the company does not keep logs, all the requests remain a confirmation of the fact that online activities of digital citizens are considered to be stored and users need to act responsibly online.

CyberGhost strongly considers that tech companies and industry leaders should address this privacy issue on a regular basis while encrypting user's data and communication and just store the necessary data to run the service.

Type of Requests

The requests have been grouped in 3 major categories:

DMCA – Digital Millenium Copyright Act complaints are usually received from various law firms representing Paramount, Sony Pictures or similar companies. These complaints usually indicate that a copyrighted material was illegally shared via a CyberGhost IP, providing details about the torrent, the date on which it was shared, the uploaders IP and the used port.

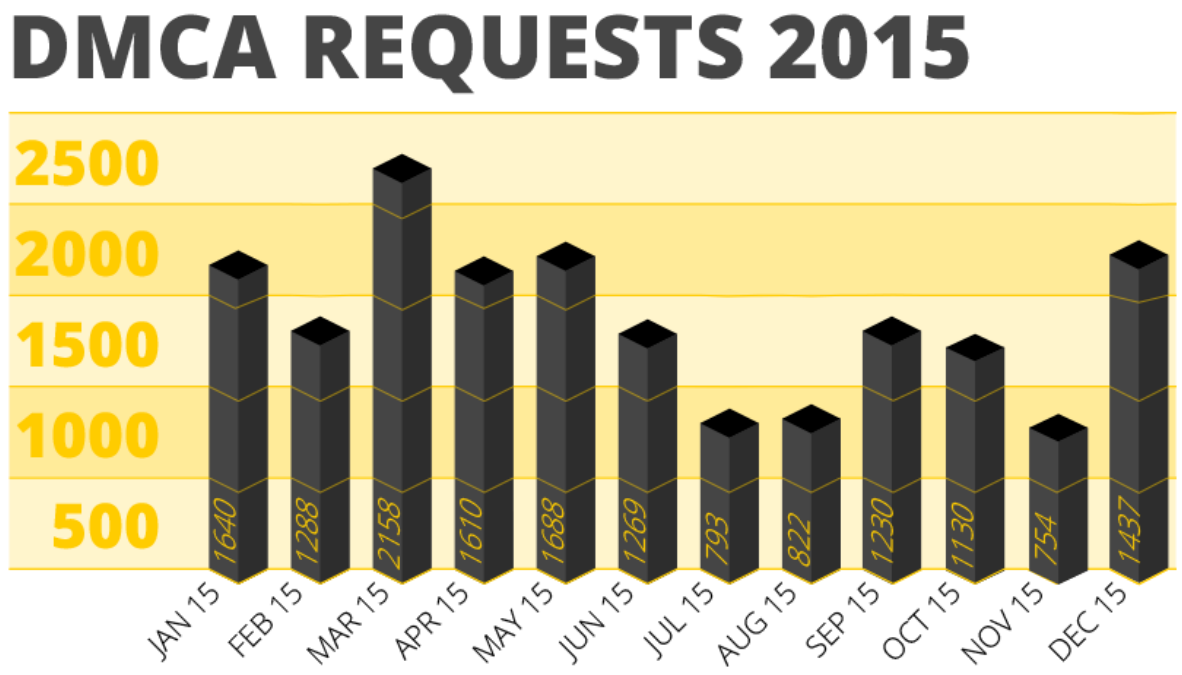
Malware Activity – Complaints are received from various parts, users receiving spams or detecting attacks from CyberGhost IPs, website owners or application developers complaining about DDoS, Botnets, Scams, log-in attempts, automated emails received from websites detecting a black listed IP address or an IP that is used for spam campaigns. CyberGhost also receives forwarded complaints from various data centers we collaborate with.

Police requests are received from various law enforcements agencies or police departments requesting logs for an IP linked to their investigation/case. These requests are usually received by the data centers and forwarded to CyberGhost.

Global Highlights

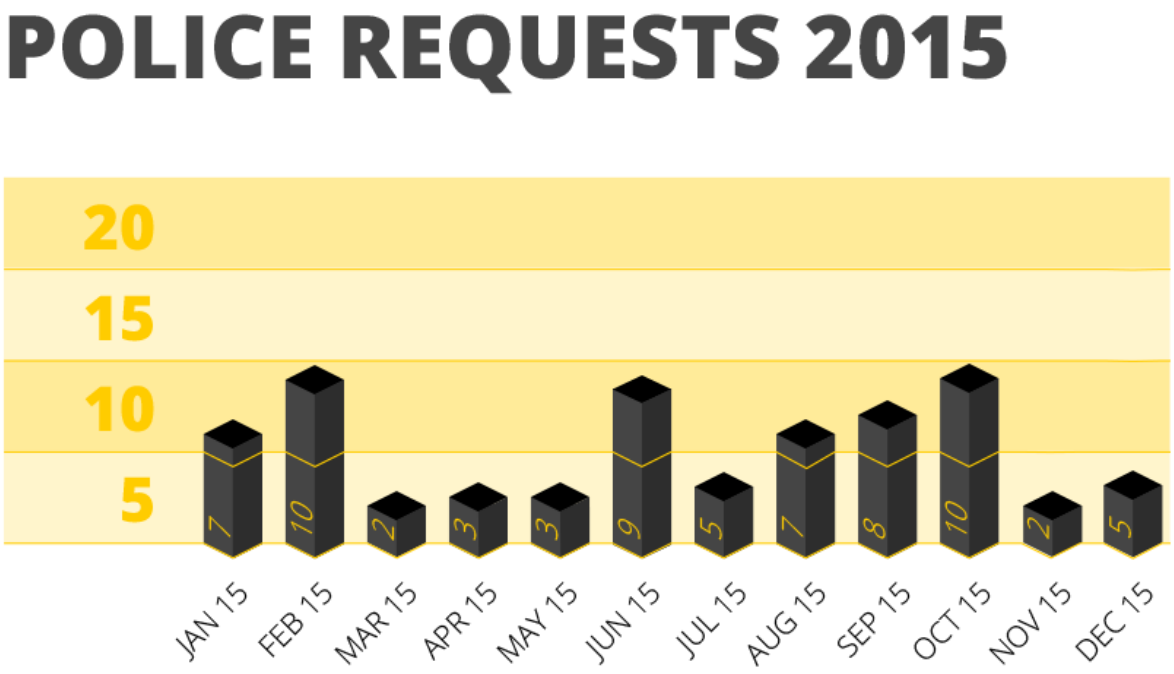
DMCA Requests

Compared to the previous year, the number of requests has decreased with an average of -21% over the past 12 months. CyberGhost received an average of 1,318 requests per month (Even though the number of users has increased with 80% from January to December 2015). The measures taken against behaviors triggering the complaints and requests are detailed in the paper. The number of DMCA complaints must also be linked to the increased activity of numerous production and distribution firms and copy right holders.



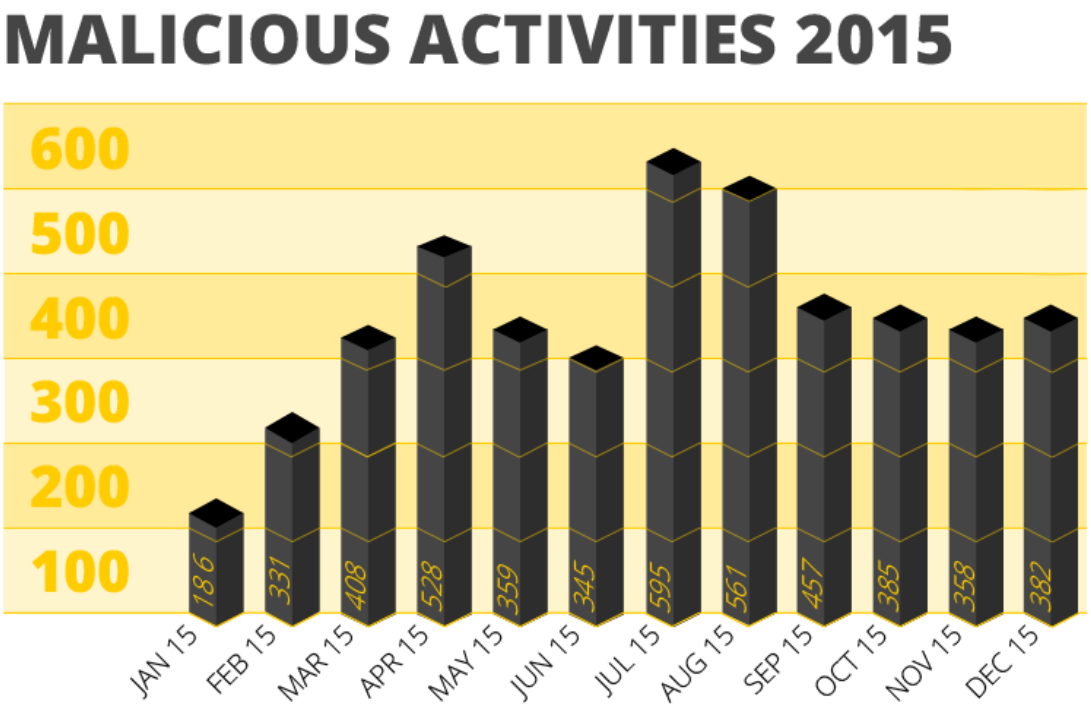
Police Requests

The increased number of users, from 3.5 million to 7.5 million has not influenced the number of police requests, on the contrary. 71 requests on disclosing user data have been counted with a monthly average of 6 demands between January 2015 and December 2015. Although the user base has seen a development of 60%, the number of received police requests has declined to -24%.



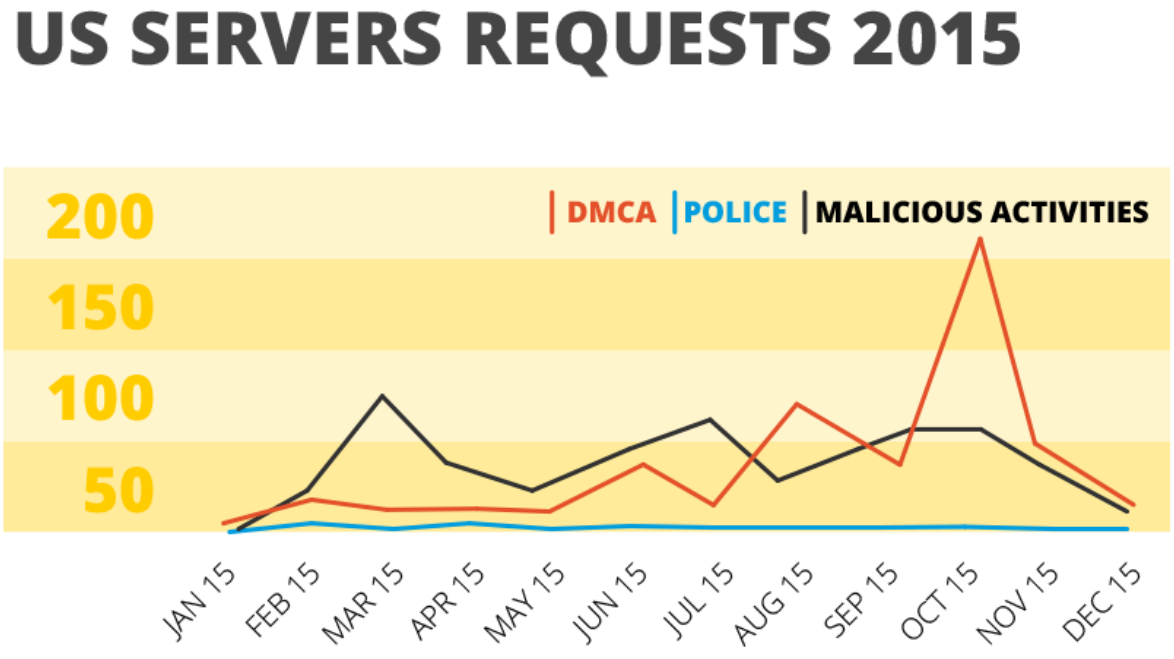
Malicious Activities

On a global scale, the reported malicious activities in CyberGhost's network have increased significantly with 310% from an average of 99 per month in 2014 to 407 per month in 2015. For the same period of time, substantial increases of malicious activities have been also reported by various security companies such as Kaspersky Lab, Trend Micro, Cisco and Symantec.



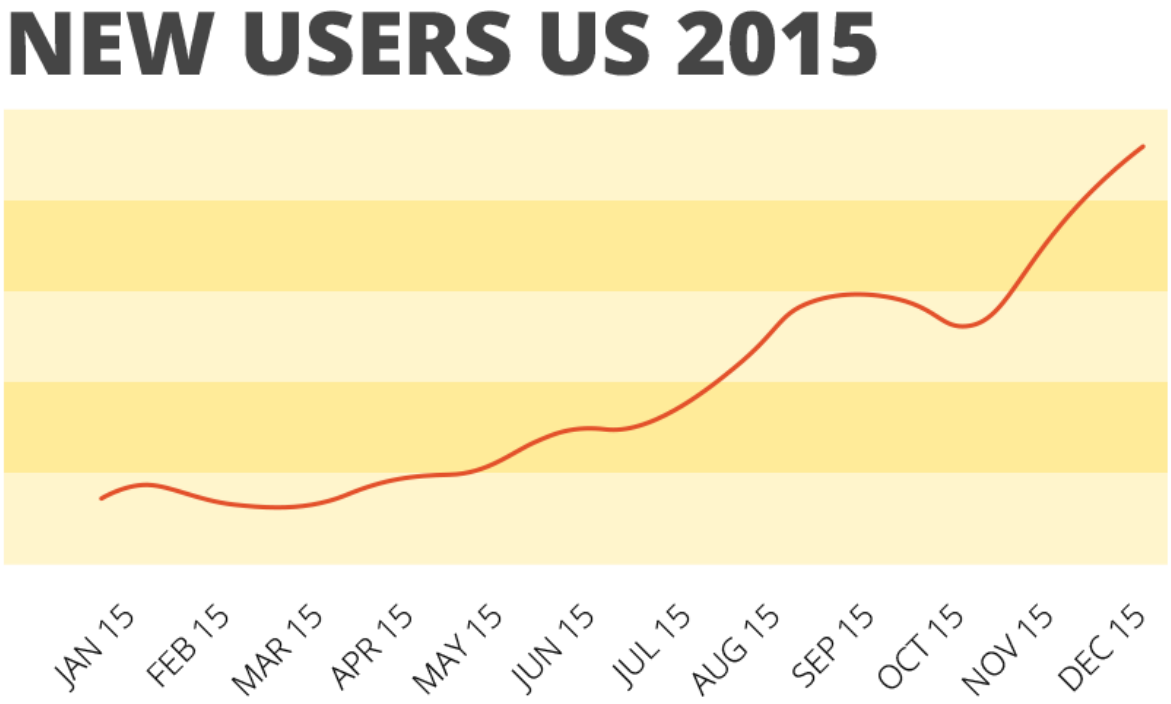
United States Highlights

New regulations with regards to censorship and mass surveillance are also a reason for the increased numbers of users. CyberGhost has observed a decline of the number of DMCA's, 59% less requests, and also 17% less police demands. As per the global development of the malware landscape, malicious activities on the U.S. servers have also risen with a substantial of 243%.



The very controversial Patriot Act was brought into public attention once again in June 2015 before the expiration date of three provisions: Section 215, the "Lone Wolf provision," and the "roving wiretap" provision. The mass surveillance-reforming USA Freedom Act has replaced it, being passed by 67 senators ending the bulk collection of U.S. phone records.[1]

In this particular case, international media, more than ever, brought into the attention of its readers the implications of such provisions, reported on NSA's activities and also highlighted the importance of privacy. All these actions can be linked to an increase of CyberGhost's U.S. more privacy aware users, as highlighted in the graphics below, reaching a growth of 150% between June and December 2015.

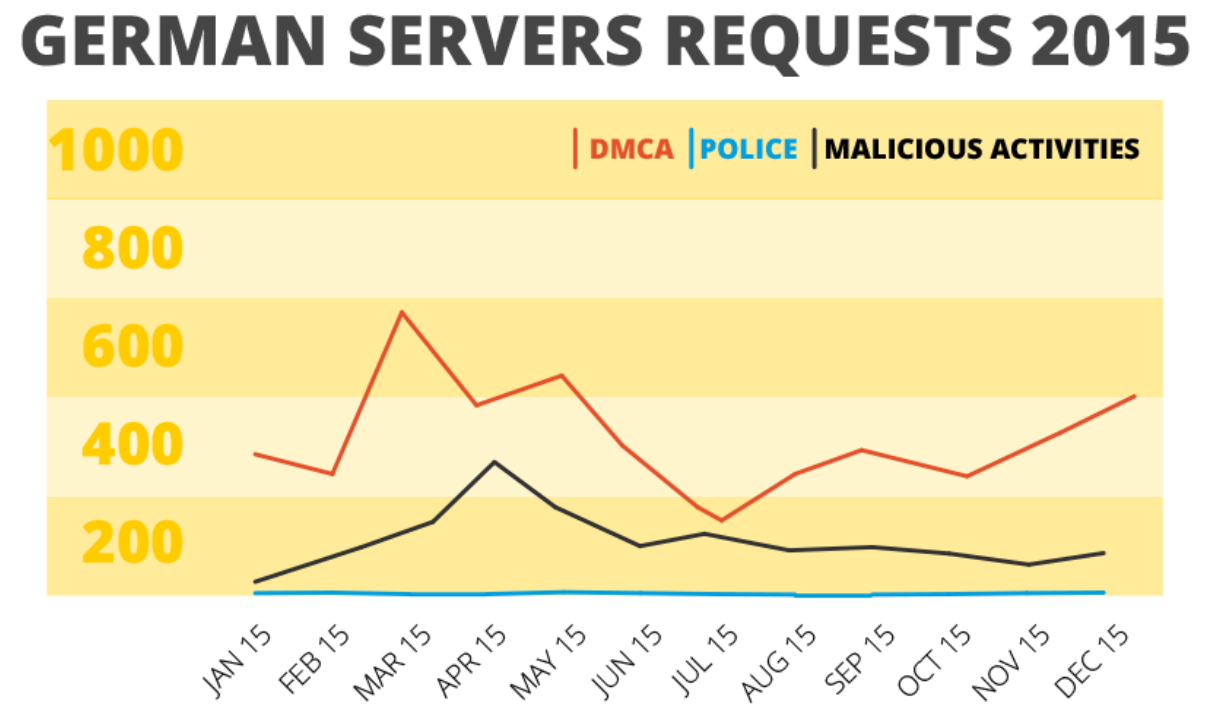


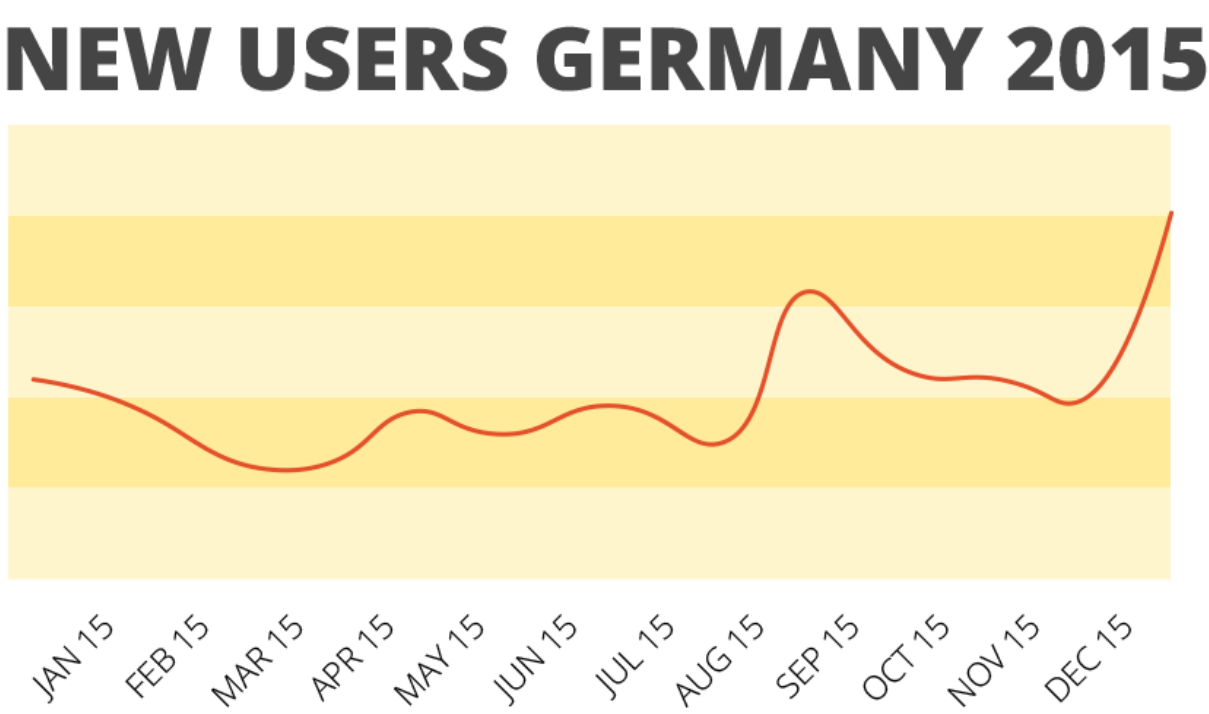
Germany Highlights

The numbers for the German servers can be easily compared to the global ones. Malicious activities have increased by 115% while DMCA demands have been 27% fewer and the police requests have decreased with 4%.

In May 2015 WikiLeaks released ten months of transcripts from the ongoing German Parliamentary inquiry into NSA activities in Germany[2], provoking massive dismay and consternation. Following this incident, Reporters Without Borders Germany (RSF Germany) took Germany's foreign intelligence agency Bundesnachrichtendienst (BND) to court. Confidential sources and whistleblowers are considered critical to the free journalistic investigations, research and reports.

[1] Http://www.usnews.com/news/articles/2015/06/02/senate-passes-freedom-act-ending-patriot-act-provision-lapse
[2] https://wikileaks.org/bnd-nsa/press/?english

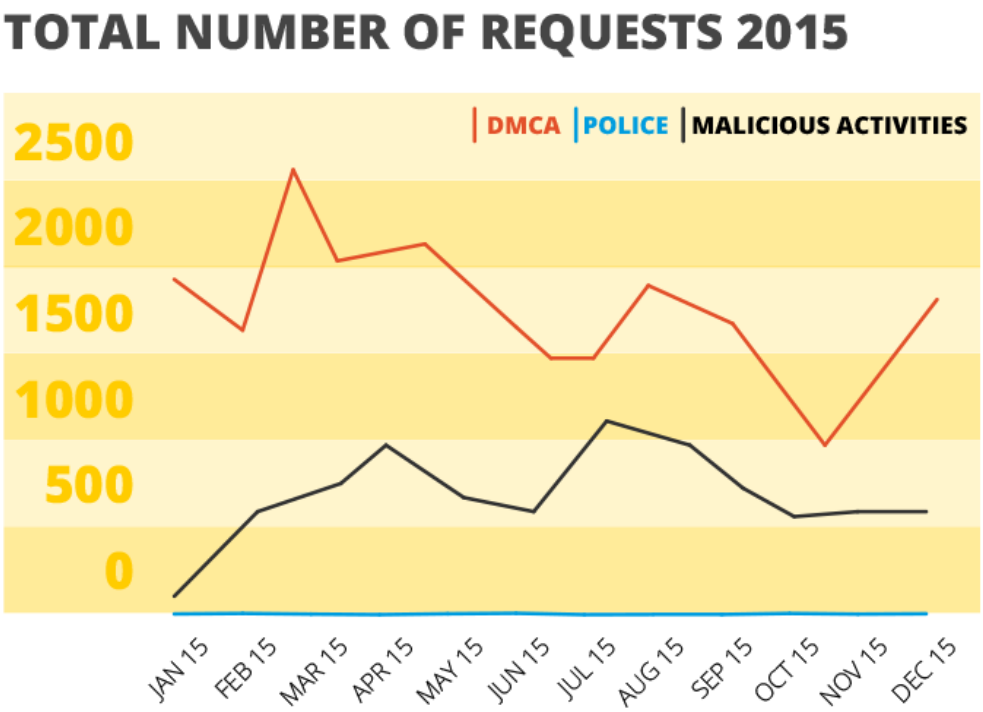




The international media exposure from June 2015 has also contributed to a higher awareness of confidentiality concerns and the right for individual privacy. It can also be linked to the increase of 60% of the German users in 2015.

Beyond the requests – a glimpse into the challenges of ensuring encryption and anonymity

CyberGhost has taken several measures to reduce the number of abuses committed on the service. Among the actions taken so far, analyzing the ports used for torrent streaming and blocking them in the countries where specific laws are in place were the most efficient. Ports in locations such as the United States, Australia, Hong Kong, Tokyo, Singapore and Mexico as well as the free servers no longer allow peer to peer connections. These measures are also linked to the pressure put on datacenter owners by various authorities to stop enabling connections to these ports.



Other measures were taken to stop the malware activities. Since most of the complaints are specifying the source of the attacks as well as the victim's IP, CyberGhost blocked access to the attacked IP so any further attack would be impossible.

Partners matter most

Collaborating with datacenters across the globe is a struggle since most of the data center owners are under constant pressure of governmental institutions and local authorities. CyberGhost does not keep logs and is unable to provide the requested data. This has led to few incidents when services of server rental to CyberGhost were rejected, most sensible situations were encountered in Russia, U.S. and Czech Republic. This is easy to understand considering that most data center owners try to avoid legal encounters or police raids ending with seizures of servers or even closing their businesses.

Censorship, governmental web filtering and mass surveillance

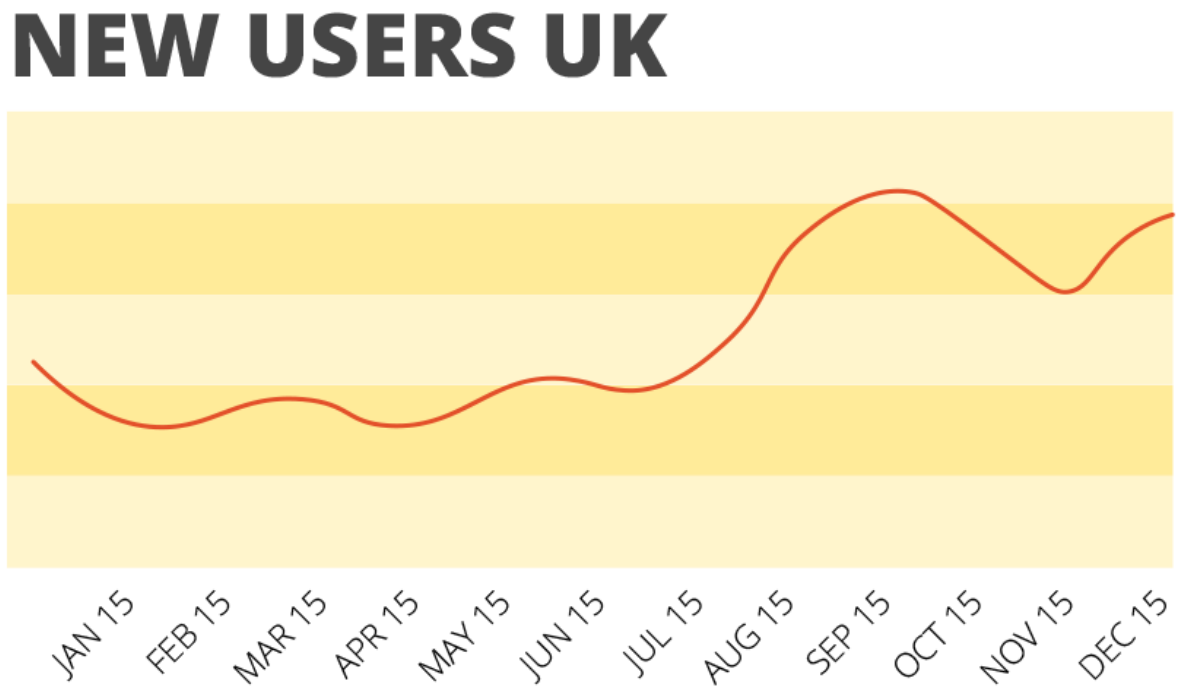
All of the above can pass as possible reasons, but at the same time we cannot have ultimate explanations why people turn to CyberGhost VPN to protect their privacy while online. Some legislation changes may be linked directly, some are just events highlighted by the international media, events that are reflected in growth of usage by country.

Censorship, governmental web filtering measures and mass surveillance awareness have also developed in the past 12 months. Whether democratic or nondemocratic countries, various legislation changes affect the online experience of users or, in some cases, influence the perception of privacy and encourage actions to encrypt communications and anonymize the online presence.

In the past year, some of the most significant law changes affected countries such as UK, Pakistan, Iran, Turkey, Russia and many others.

UK: Court-ordered blocks

Although no censorship related law was passed during the past 12 months, 'Section 97' allows right-holders in the UK to require ISPs to block copyright-infringing sites[3] when presented with court orders. Since the court orders are not made public[4], "over blocking" is sometimes reported and can lead to blocking “clean” websites.



[3] http://www.revk.uk/2013/11/section-97a-orders.html
[4] http://www.ispreview.co.uk/index.php/2013/08/open-rights-group-uk-pushes-for-isp-website-blocking-orders-to-be-public.html

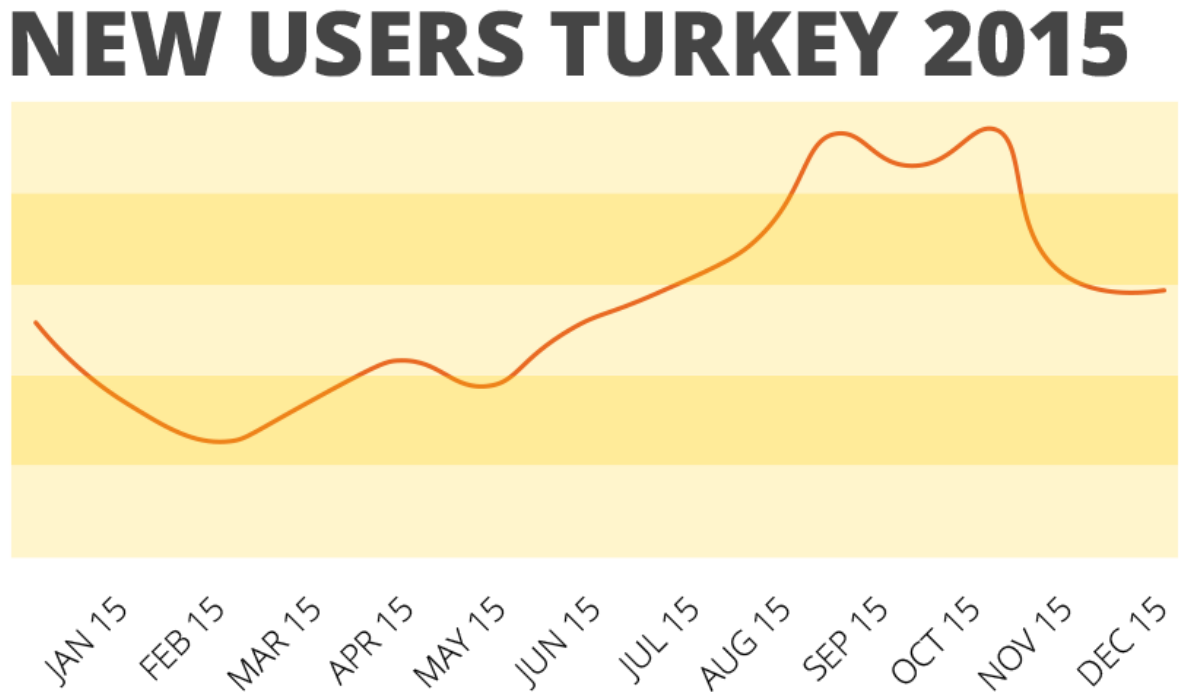
TURKEY

In the past 12 months, various happenings have been reported by the international media that have been reflected in user behaviors and increase. The law passed on the 5th of February 2014 by the Turkish Parliament[5] has allowed the telecommunications authority (TIB) to block any website within 4 hours without first seeking a court ruling; and requires Internet providers to store all data on web users' activities for two years and make it available to the authorities upon request.

In 2015 there were several Twitter bans by the Government, such as the one in 22th of July 2015, to be removed by court order, only after Twitter agreed to remove images related to a suicide bomb attack that took place in Turkey's Southeast. These temporarily social media bans occur periodically here.

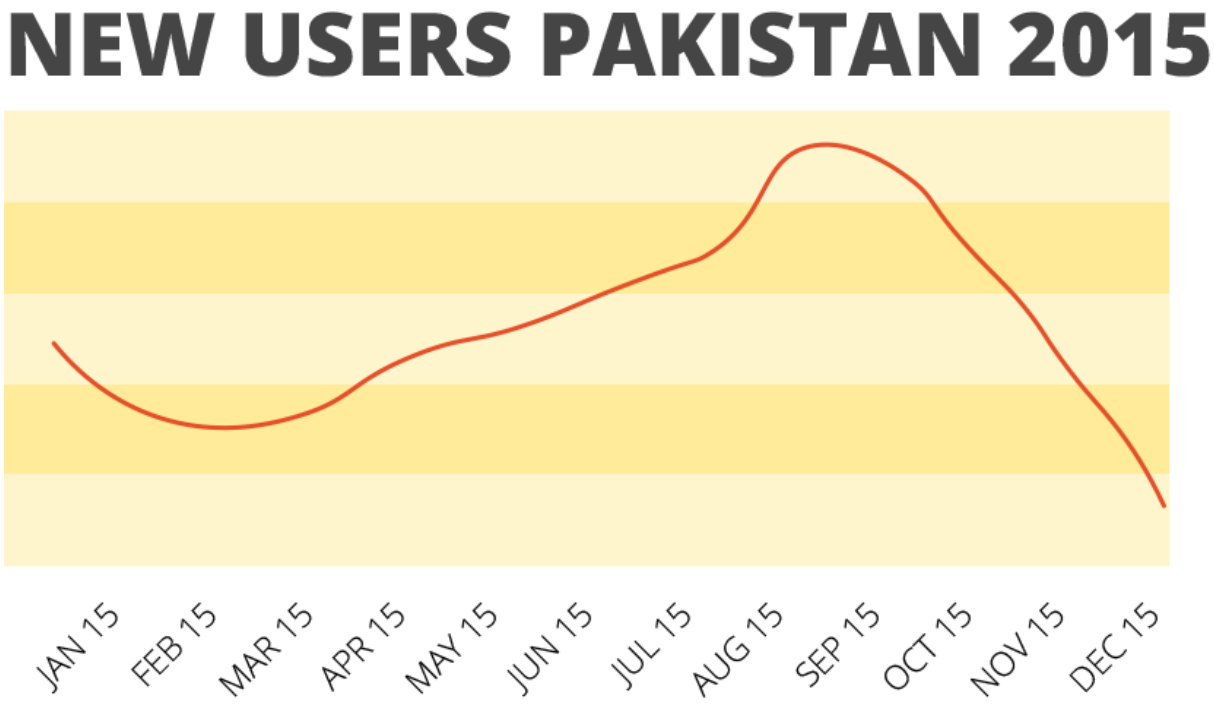
In April 2015, the list of blocked Internet sites maintained by the monitoring website Engelli Web contains over 78,000 domain names.[6]

In the light of these events, the increase of the Turkish users is one of the highest among CyberGhost users reaching a growth of 68% in 2015.



Pakistan has seen the highest user base growth rate, 73% increase in just six month, from March to August 2015. One reason linked to this increase of users might also be the ban of the WordPress platform, considered a National Security threat and banned by the Pakistan Telecommunication Authority (PTA) in March 2015[7].

[5] https://freedomhouse.org/report/freedom-net/2013/turkey
[6] http://engelliweb.com/
[7] http://techcrunch.com/2015/03/22/wordpress-blocked-in-pakistan/



Russia was also impacted by severe censorship actions. Among them, one incident was in June 2015, some ISPs blocked the 485 billion web pages, basically the Internet Archive. The measure followed after an order to censor a page contained within, allegedly advocating "extremist" material. The Russian government went even further in August 2015 and briefly banned Wikipedia after the site refused to delete a webpage containing information on how to prepare and use charas, a form of cannabis. Wikipedia was accessible a few hours later when the webpage with „online content about drug use" was removed.

Bitcoin was also in the visor of the governmental censorship because "it contributes to shadow economy".[8] This led to the block of bitcoin.org and other Bitcoin related websites.

The money issue

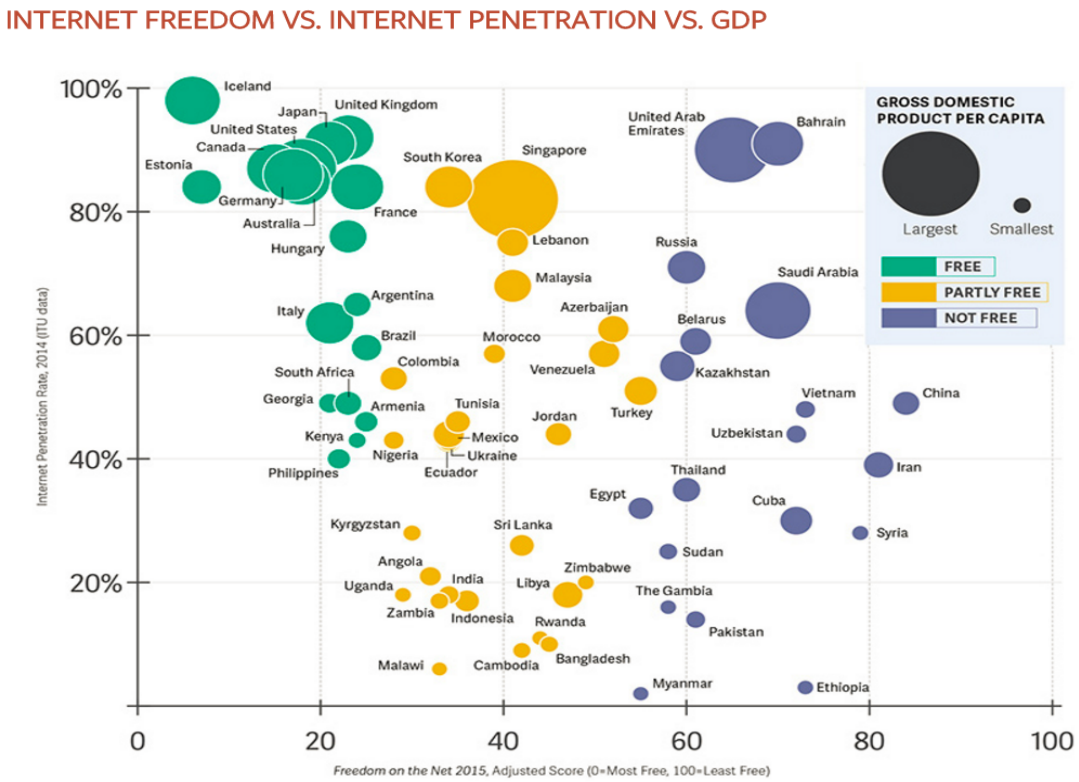
The top ten countries where CyberGhost is used is also divided into two categories: the paying customers are the top 4 countries (net medium income for Germany - 2,315 €, U.S. - 2,360 €, Great Britain - 2,810 €, France - 2,223 €) versus the other 6 countries of the top where the average net income per year is 350 €[9] (Russia, Nigeria, Iran, and Pakistan)[10] and where people use our free service.

These data show a balance between users enjoying a very fast service and access to more than 650 servers across the globe supporting the access of users in most countries

[8] http://www.newsbtc.com/2015/01/13/russia-blocks-bitcoin-sites/
[9] https://en.wikipedia.org/wiki/list_of_countries_by_average_wage
[10] http://www.tradingeconomics.com/russia/wages

with human rights issues that don't have the economical means to afford to pay premium subscription. CyberGhost free service is based on the contribution of the most developed countries in the world.

The recent study published by Freedom House.org in October 2015 "Freedom on the Net 2015"[11] has created a map based on "internet freedom scores", Internet penetration and GDP.



Is privacy a personal matter?

In correlation to our transparency report is also the concern of privacy. Measures educating the public with regards to online safety must be linked to the VPN usage. Multiple organizations have launched various programs such as: The BC AWARE Campaign for Privacy & Security Awareness[12], Data Privacy Day by www.staysafeonline.org where CyberGhost was also a partner in 2013 for "Respecting Privacy, Safeguarding Data and Enabling Trust"[13] supported by Homeland Security[14], Privacy Awareness Week, initiative of Asia Pacific Privacy Authorities forum (APPA) and supported by Office of the Privacy Commissioner of Canada[15] and many other campaigns. They all have the goal to instruct their public about the importance of privacy. Some of these campaigns are supported by governmental institutions around the globe…

[11] https://freedomhouse.org/report/freedom-net/freedom-net-2015
[12] http://www.bcaware.ca/about-us/why-this-campaign/
[13] https://www.staysafeonline.org/
[14] http://www.dhs.gov/national-cyber-security-awareness-month
[15] https://www.priv.gc.ca/information/paw/index_e.asp

Can privacy be measured?

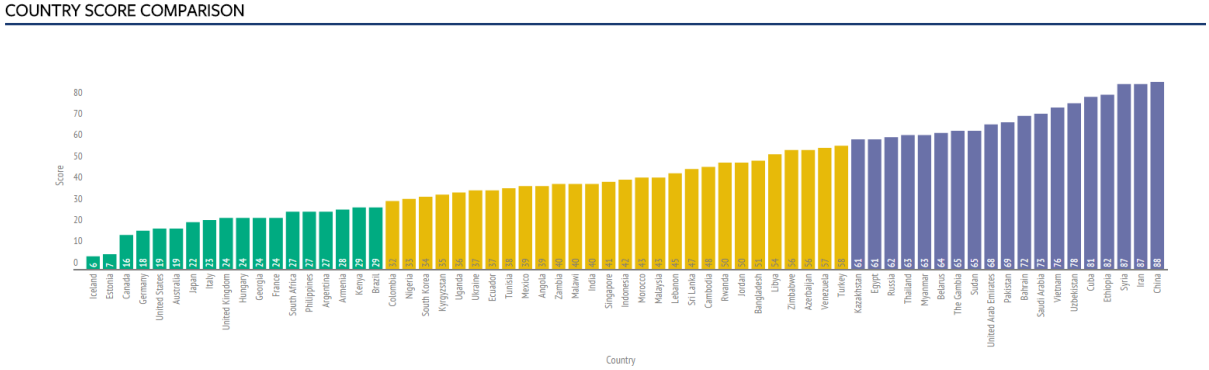
Although privacy has different understandings on personal/cultural level, there are several rankings of privacy laws by countries, each receiving various "scores" such as:

- BackgroundChecks.org created the "privacy scoreboard," which takes into consideration whether a country's government has privacy laws, if Internet is restricted in any way, if it is known that the government uses spyware, if government protects free speech, and other metrics. Based on that criteria, some of the best places for privacy include Spain+50, the Czech Republic+50, Iceland+50, Norway+50, and Slovenia+40, according to BackgroundChecks.org. On the other end of the scoreboard are Bahrain-25, Iran-25, Nigeria-20, Syria -20, and Malaysia-20.

- Also DLA Piper measured the regulations of each country. The analysis DLA Piper of data protection laws is placing Canada, Germany, France, Sweden, Norway and various other European with heavy regulation and enforcement. USA, Australia and Argentina are considered under robust regulation and enforcement, while Russia, Ukraine, South Africa and Mexico are considered moderate.

- According to the Global Consumer Sentiment Survey made by the Boston Consulting Group in 2013[16], the question "How private do you consider the following types of personal data?" respondents from Germany, France, Spain, Canada, Australia, and the U.S. cared the most about credit card data, financial data, information about children and health genetic information.

- Freedom House has recently published the Freedom on the Net 2015, a report that elaborates the actual stage of internet freedom around the world considering it in decline for a fifth consecutive year „as more governments censored information of public interest while also expanding surveillance and cracking down on privacy tools"[17]



[16] https://www.bcgperspectives.com/content/slideshow/information_technology_strategy_digital_economy_data_privacy_by_the_numbers/#ad-image-0

[17] https://freedomhouse.org/report/freedom-net/freedom-net-2015

The data mentioned above show that citizens in these countries are more aware of privacy and take various measures to increase their online privacy. On the other pole, users in nondemocratic countries need online security of their online identity. The regulations and privacy laws changed on the last decade must be linked to such behaviors.

Encryption: Our digital weapon we should all use

The transparency report published by CyberGhost is aimed to inform about the various requests and raise awareness of the actual fact that online citizens are being watched, monitored and even traced. Everyone that goes online should consider encryption as an ultimate weapon to protect their identity.

The revolution of the digital and technologized world begins with us and the measures we take to protect our identities. Our weapon in these digital times is encryption. Julian Assange: “Cryptography is the ultimate form of non-violent direct action”.

Encrypting communication on every level is key in securing online users. No matter if we talk about sensitive financial information, personal medical data, identity theft, journalistic research on very sensible topics or persons in nondemocratic countries informing themselves or expressing opinions online; data must be encrypted. Encryption is the only way digital citizens can protect themselves.

We want to enforce the statement that surrounds all our activities: CyberGhost does not log any online activity of any users. Privacy is the core business and CyberGhost’s mission. CyberGhost stands for freedom of the Internet worldwide! We want to enhance freedom of speech, access to a censorship free Internet and research on the uncensored Internet.

Calling up the Tech Industry

We advise on agreeing on a standard transparency report in the tech industry highlighting relevant data for users not for companies. We all need to be able to differentiate noise from signal! Since some of the transparency reports only mean a new PR campaign for some tech companies, we invite EFF and other organizations to mediate and work together with all willing tech companies to agree on a standard report comparing similar data. We are looking forward to various collaborations with other companies to ensure a standard on transparency reports and really make a change based on telling the truth.

References:

Http://www.usnews.com/news/articles/2015/06/02/senate-passes-freedom-act-ending-patriot-act-provision-lapse
https://wikileaks.org/bnd-nsa/press/?english
http://www.revk.uk/2013/11/section-97a-orders.html
http://www.ispreview.co.uk/index.php/2013/08/open-rights-group-uk-pushes-for-isp-website-blocking-orders-to-be-public.html
https://freedomhouse.org/report/freedom-net/2013/turkey
http://engelliweb.com/
http://techcrunch.com/2015/03/22/wordpress-blocked-in-pakistan/
https://antizapret.info/site.php?id=5244
http://techcrunch.com/2014/12/03/github-russia/
http://www.newsbtc.com/2015/01/13/russia-blocks-bitcoin-sites/
https://en.wikipedia.org/wiki/list_of_countries_by_average_wage
http://www.tradingeconomics.com/russia/wages
https://freedomhouse.org/report/freedom-net/freedom-net-2015
http://www.bcaware.ca/about-us/why-this-campaign/
https://www.staysafeonline.org/
http://www.dhs.gov/national-cyber-security-awareness-month
https://www.priv.gc.ca/information/paw/index_e.asp
https://www.bcgperspectives.com/content/slideshow/information_technology_strategy_digital_economy_data_privacy_by_the_numbers/#ad-image-0
https://freedomhouse.org/report/freedom-net/freedom-net-2015