# SWITCHcert Security Report

April 2014


SWITCH

## I. On NSA and the Big Players

For most American internet tech companies, damage control is the order of the day, ever since a majority of them were outed a few months ago as more or less willing NSA accomplices. In an effort to win back miffed business and private customers, the big players such as Apple, Google, Facebook, AOL, Microsoft, Yahoo and IBM are investing a lot of time and money into PR work. Facebook founder Mark Zuckerberg for example informed the 1.2 billion users of Facebook that he was «confused and frustrated», and that he had personally filed his complaints with President Obama about the NSA's activities.

Google CEO Larry Page rolled up a mix of pathos and practical responses, promising a double encryption standard for Gmail through HTTPS and server-to-server encryption. Page also informed the net community at TED Vancouver that he was seriously concerned about Google's main mission, free access to information: «I don't think we can have a democracy if we have to protect our users from the government [and] from stuff that we never had a conversation about […] we need to know what the parameters of it is, what the surveillance is going to do, and how and why». Sadly, Page wasn't able to explain the difference between good and bad online surveillance.

IBM still vehemently denies any involvement in NSA activities. IBM's head legal representative, Robert Weber, penned an open letter firmly stating that the company has never shared client information or unlock codes, nor built in back doors for government investigators to use.

Surprisingly, Yahoo – one of the few big players to cooperate with the government only after explicit court orders – has been very low-key about the whole affair and their involvement with the NSA.

### Internet Giants Collecting Own User Data

Rajesh De, head of the NSA legal department, isn't convinced by the tech companies' grandstanding. In front of the Privacy and Civil Liberties Oversight Board of the US Senate, De claimed they all knew about the investigations and even fully cooperated in the search for specific meta and communications data of individuals as well as the general monitoring of the net, writes the Guardian newspaper.

The double standard is clearly on display elsewhere as well – the German IT forum Heise has investigated the data protection agreements of various American email providers such as Microsoft, Apple, Google or Yahoo and determined that while they condemn the NSA for aggressive investigation methods, they also all openly state they may do the same, or pass the data to third parties.

### NSA Hunting for Last 1.2 Billion Data Sets

Rumor has it that the NSA currently manages something around 6 billion data sets of meta data. Considering the world population of 7.2 billion people, NSA is on track to monitor every single individual on Earth, even though the majority only uses the web for emails or phone calls. The data sets are probably shared between the Big Five security services – Great Britain, Canada, Australia and New Zealand. James Clapper, American Director of National Intelligence, also recently admitted that legal loopholes were exploited to eavesdrop on citizens without legal permission to do so. He also conjoined data collection and analysis – if one is legal, why not the other?

In slightly more positive news, President Obama may soon put an end to the systematic collection of data on American telephone communications – the monitoring will soon be done not at the NSA, but directly at the telecommunications providers.

Find out more:

http://gmailblog.blogspot.de/2014/03/staying-at-forefront-of-email-security.html
http://www.politico.com/story/2014/03/barach-obama-tech-ceos-nsa-104881.html

http://asmarterplanet.com/blog/2014/03/open-letter-data.html
https://www.facebook.com/zuck/posts/10101301165605491?stream_ref=10
http://www.theguardian.com/world/2014/mar/19/us-tech-giants-knew-nsa-data-collection-rajesh-de
http://www.mobilegeeks.de/vertrauen-zerstoeren-dafuer-brauchen-wir-die-nsa-nicht/
http://www.nzz.ch/aktuell/international/auslandnachrichten/nsa-sammelwutsoll-gebremst-werden-1.18270453
http://futurezone.at/meinung/ueberwachen-koennen-wir-am-allerbesten/57.970.001
http://www.golem.de/news/geheimdienste-nsa-faengt-irakische-kommunikationsdaten-komplett-ab-1404-105521.html
http://www.wyden.senate.gov/download/?id=130BFF88-A3C0-4315-A23B-C4F96C499D9D&download=1

## II. European Court of Justice Permits Internet Censorship

European politicians are concerned about the developing situation in Turkey. But the situation inside the EU may be just as worrying – at a time when Europe is upset about censorship and internet access restrictions in Turkey, the European Court of Justice in Luxemburg recently approved the implementation of government-controlled internet censorship filters. Internet activists fear the ruling will lead to state media censorship across the EU.

Internet providers in the EU will soon be required to block access to content if it violates intellectual property laws in any EU member state. The precedent was set after Austrian provider UPC Telekabel Wien refused requests by «Filmverleih Constantin» to block users from the streaming website kino.to.

### The Dream of Good and Bad Censorship

«Der Spiegel» reports that the movie industry is already requesting blocks for specific websites all across Europe. In Germany, the idea of blocking websites was turned down, the approach instead focusing on deleting the content in question. Based on a list of requested website blocks, the Swiss entertainment industry would very much like a legal precedent similar to the EU, according to the Chaos Computer Club Zurich (CCCZH). The long and varied list contains a number of illegal streaming and download sites. CCCZH's issue with the list: «There is no good or bad censorship. […] Every form of censorship leads to abuse.»

A typical and current example of this is a recent video of an American diplomat ranting about the EU, called «Fuck the EU». The video in question is well-known and widespread – but on the computers of German government employees, it is blocked. «Either there is content you can't see because it's illegal. Then you have to delete it.

Or it's legal content, then there is no reason to block it», said a representative of the German left wing. After being asked about the video in question and the censorship at play, the German federal government has requested time for consideration.

Find out more:

http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-03/cp140038de.pdf
http://www.anwalt24.de/beitraege-news/fachartikel/europaeischer-gerichtshof-provider-muessen-illegale-seiten-sperren-das-freie-internet-ist-gefaehrdet
https://www.ccczh.ch/News
http://www.heise.de/tp/artikel/41/41402/1.html

## III. Zuckerberg Gambling on Virtual Reality

After paying 19 billion USD for WhatsApp, Facebook's most recent acquisition is certainly cheaper, but far more interesting. Zuckerberg and his social network giant laid out 2.3 billion USD for virtual reality developers Oculus VR, makers of the 3D headset Oculus Rift. While only a few prototypes exist, the concept of Immersive Gaming had the video game enthusiasts hooked on the startup. So what does Facebook plan to do with the company?

According to Zuckerberg, headsets like the Rift will be the future of online communication. On his Facebook page, Zuckerberg explained how the device gives you the impression you're actually in a different place with other people, and how he thinks the technology could revolutionize everyday life.

### Crowdfunding via Kickstarter Gets Oculus Rolling

Prior fans of the gaming headset aren't convinced, and for good reason – a portion of the money used to develop Rift came from them. In 2012, the Oculus VR team presented a rough prototype on Kickstarter, but the hype was enough to generate over 2.5 million USD in donations. Internet activists are now upset that a crowdfunded startup would sell out to a major tech company.

Zuckerberg's vision for Oculus includes «[…] the potential to be the most social platform ever. Immersive, virtual and augmented reality will be part of people's daily lives». Examples include virtual movie visits with a partner, virtual classrooms or medical consultations - though the question of who would willingly send medical information over the internet remains.

### Google Glass Compromised

Security is also a big concern for virtual reality headsets. Google Glass, a competitor product of sorts, recently made headlines after reports of security flaws emerged. Two students from California, Mike Lady and Kim Paterson, showed that Google's policy for Glass apps isn't a hindrance for cyber criminals. Their Glass app called Malwarenotes claimed to help with note taking, but in fact took clandestine pictures of the environment every 10 seconds and transmitted them to possible attackers – all without the wearer's consent or knowledge. Glass owners are warned not to leave their Glasses unattended.

Google's defense: the virtual reality glasses aren't a mainstream product and the flaw in question isn't «major». In light of this attitude to security and the fact that there are no hardware-side security measures in Glass, it's no surprise that more and more «No Glass» zones are popping up across the USA. Ironically, Kim Paterson will end her studies this spring and then start her new job at… Google.

Find out more:

http://www.oculusvr.com/blog/oculus-joins-facebook/
https://www.facebook.com/zuck/posts/10101319050523971
http://www.nytimes.com/2014/03/26/technology/facebook-to-buy-oculus-vr-maker-of-virtual-reality-headset.html
http://www.forbes.com/sites/andygreenberg/2014/03/18/researchers-google-glass-spyware-sees-what-you-see/
https://www.kickstarter.com/projects/hellobragi/the-dash-wireless-smart-in-ear-headphones
http://www.forbes.com/sites/andygreenberg/2014/03/18/researchers-google-glass-spyware-sees-what-you-see/

## IV. Turkish Government Bans YouTube and Twitter

Since 2011, Turkish Prime Minister Recep Tayyip Erdogan has been continually limiting internet access in his country. But in March, he stepped it up a notch and quickly blocked access to both short messaging service Twitter and video streaming site YouTube. Both, according to Erdogan, are a danger to Turkey. Additionally, both platforms apparently didn't react to content removal orders from Turkish courts for «continuing insults».

Of course, both platforms are also very popular media channels for Turkish opposition movements and civil rights groups. At first, it was easy to circumvent the government censorship by using Google's free DNS service. However, since late March, Turkish telecommunications providers are apparently forwarding requests for the IP addresses of Google's DNS servers to their own DNS servers, from where users are re-directed to fake sites.

### Today Twitter, Tomorrow the World Wide Web

Currently, if Turks want to access YouTube or Twitter, they are re-directed to a government-controlled site. Security experts from the American company Renesys warn that this site could be used to monitor the entire population's surfing behavior or manipulate/hijack their computers. The recent changes cast a shadow over the future as well – today YouTube, tomorrow Gmail or Dropbox. Renesys also mentions the economical damage for Turkey, a country trying to grow in an internet-dependent world economy. Foreign investors, companies and citizens will certainly find it harder to trust the Turkish net infrastructure now.

Find out more:

http://www.nzz.ch/aktuell/international/auslandnachrichten/die-tuerkische-regierung-blockiert-youtube-1.18272248
https://blog.twitter.com/2014/victory-for-free-expression-in-turkish-court
http://www.heise.de/mac-and-i/meldung/Bericht-Belgischer-Richter-zog-Web-Sperre-gegen-Apple-in-Betracht-2133804.html
http://www.renesys.com/2014/03/turkish-internet-censorship/
http://www.spiegel.de/netzwelt/web/erdogan-laesst-surfer-in-die-irre-klicken-a-961757.html
http://googleonlinesecurity.blogspot.de/2014/03/googles-public-dns-intercepted-in-turkey.html

## The Clipboard: Interesting Presentations, Articles and Videos

Why do web applications have so many flaws, but never undergo testing for security weaknesses? Jeff Williams, a specialist for software development and security, examines the underlying issues and presents three recommendations to improve the situation:

http://www.darkreading.com/application-security/flying-naked-why-most-web-apps-leave-you-defenseless-/d/d-id/1127875

One year after «APT1», Kevin Mandia provides an update on what has happened so far and explains what organizations should do to reduce their security gap:

http://www.fireeye.com/blog/corporate/2014/04/apt1-the-state-of-the-hack-one-year-later.html

ReVuln security experts show the downside of the Internet of Things by compromising a Philips SmartTV and then collecting sensitive data:

http://securityaffairs.co/wordpress/23523/hacking/philips-smarttv-susceptible-serious-hack-according-revuln-experts.html