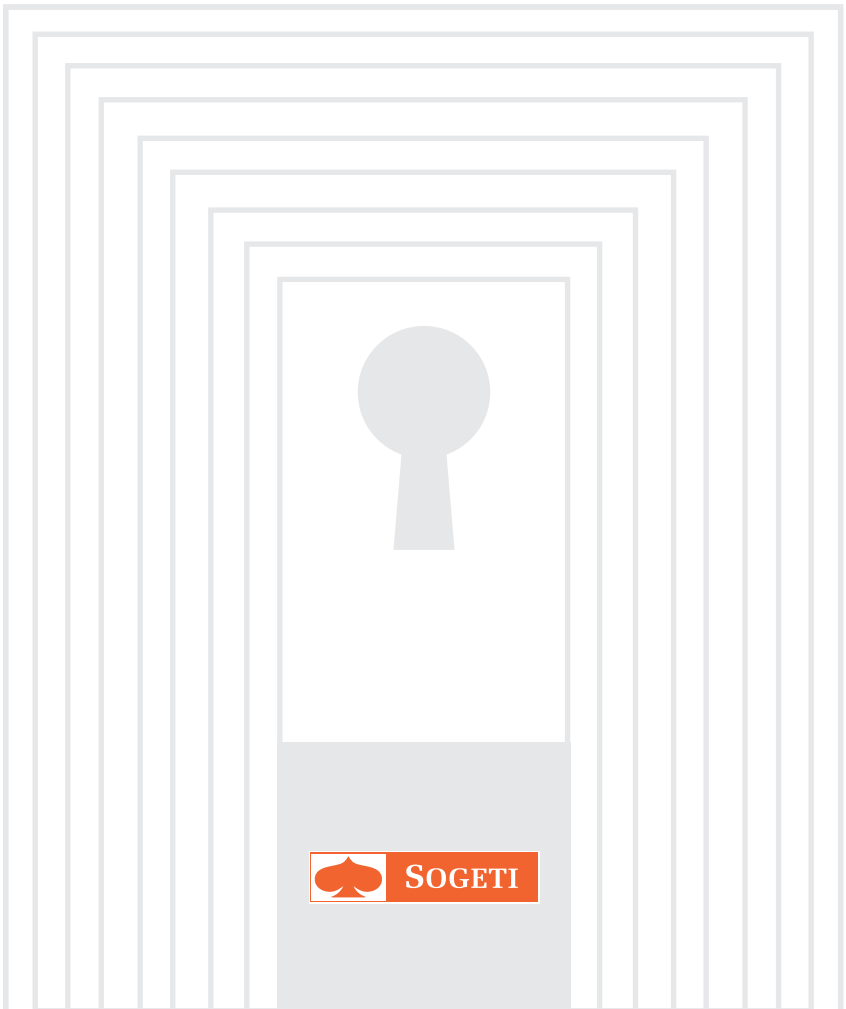
03

SOGETI : INSIGHT ON INNOVATION

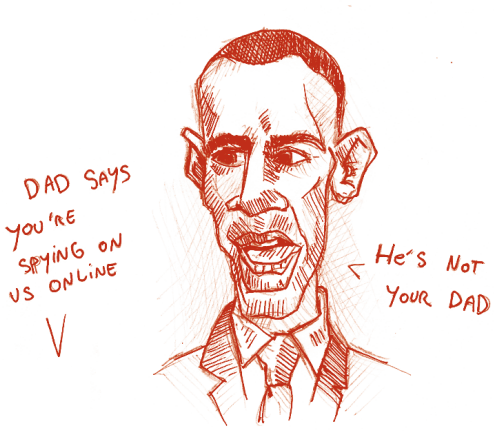
The Year Privacy Died



This is the year of privacy, or the lack of it. Some say the death of it. This is the year in which secret agencies lost their secrets. Thanks to Edward Snowden, now everybody knows what some have said for a long time: we're being watched constantly. A popular joke on Facebook describes this state of privacy ironically. A young boy is having lunch, sitting next to President Obama, and he says to him, "Dad says you're spying on us online". Obama responds, "He's not your dad." An interesting question to ask is what the long term consequences of what this public awareness looks like. In fact, there are signs that this could dramatically impact the cloud service industry.

> ***"Private telephone calls, web behavior, and our digital lives are easily accessed by tens of thousands NSA employees"***

Private telephone calls, web behavior, and our digital lives are easily accessed by tens of thousands NSA employees. "Beyond Orwellian", "Nightmarish" and "The Exxon Valdez of the Internet" were some of the reactions. Everybody is shocked, even those who say we could have known that secret agencies work like this. They are shocked because of our ignorance and naivety. Some are shocked by the fact that public and private companies work together so closely. It's a perfect storm for the creation of a surveillance nation. The difficulty for many of the companies involved is to keep or regain the trust of the public. Can you "privacy-by-design" yourself out of this situation, when sarcasm, irony and anger control the debate?
On the other hand, at least there's a debate. This is what many of the companies, like telecommunication providers, were asking for a long time. And, they seem happy; not because of the raise of distrust, of course, but because now it can be more openly be discussed, there's no taboo anymore. Perhaps that will be the most important long term impact on society.



Now that we all know, what do we do with it?

Should we accept the surveillance nation, and is there anything we can do about it?

What checks and balances or secret agency governance do we need, and will it work?

These questions need to be addressed, but there are no easy answers. And it's probably too early to tell. Meanwhile, one of the practicalities is the potential loss of business by US and UK cloud providers. Let's focus on that, but first have a look on how secret agencies work.
"Everybody is shocked, even those who say we could have known that secret agencies work like this. They are shocked because of our ignorance and naivety."

HOW SECRET AGENCIES WORK

Prism is the US surveillance program that allows the NSA to access the accounts of major US cloud services providers. This includes the accounts of non-US citizens. The US government has struggled to respond to the series of revelations in the Guardian newspaper about the extent of the NSA's oversight of data, which travels into the US. Prism allows it to target details about individuals residing outside the US; the NSA claims that it has "direct access" to data from Google and Microsoft, among others, who are both also major cloud computing providers. The two companies have denied that the NSA has direct access but said that they allow "lawful" transmission of data to it.

Another joint-program between X,Y,Z is Xkeyscore, which allows the NSA and partners in Australia, New Zealand, England and Canada to drill down to details about individuals almost anywhere on the internet.

Here are the other US companies involved by "PRISM scandal," and the dates PRISM collection began for each provider (taken from the slide deck that Edward Snowden handed to the news papers):

Another special NSA project called "Sigint enabling" plays an important role in this public-private collaboration. Sigint is a $250 million-a-year program that works with Internet companies to weaken privacy by inserting back doors into encryption products. From an excerpt from the 2013 Intelligence Budget request on the website of the New York Times we read, "The Sigint Enabling project actively engages the US and Foreign industries to covertly influence and/or overtly leverage their commercial product designs."

This enabled the NSA, for instance, to crack commonplace internet encryption that is used in email and financial transaction encryption. A few weeks after the revelation of Prism, Edward Snowden revealed another backdoor project called Tempora. On 21 June 2013, the Guardian reported that the English secret service GCHQ had placed data interceptors on fiber-optic cables that carry internet data in and out of the UK. This is known as "up-stream" data collection. The NSA uses both routes, according to one of the slides of the "official" deck of Snowden. The maxim is: "You should use both".

According to the Guardian, these UK-based fiber optic cables include transatlantic cables that carry internet traffic between the US and Europe, meaning that GCHQ is able to directly access large amounts of global internet data. The documents Snowden revealed show GCHQ's surveillance gives it the "biggest internet access" out of the "five eyes," which consist of spy agencies in Australia, New Zealand, the UK, Canada and the US, the same agencies involved in Keystone. Based on all the documents and articles in the news papers, Ashkan Soltani, an independent privacy researcher and consultant, along with another researcher, nicknamed "semipr0," made an infographic that shows how secret agencies may work:
In the box on the left at the top there's the NSA Analyst. Between them, the GCHQ and NSA have 550 analysts poring over the data — and 850,000 people with top secret clearance can access it.

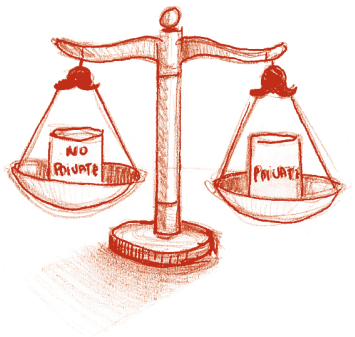
IS ENDING PRIVACY A GOOD IDEA?

Glenn Greenwald, journalist of the Washington Post that worked on the Prism case, said to a reporter of CNN that the ambition of the NSA is to end privacy:

"There is a massive apparatus within the United States government that with complete secrecy has been building this enormous structure that has only one goal, and that is to destroy privacy and anonymity, not just in the United States but around the world."

Another article from Glenn Greenald and Jacues Follorou, published in Le Monde, claims that 70.3 million recordings from French citizen were collected from December 2012 to January 2013, and that the NSA's surveillance system apparently also "picks up SMS messages and their content using key words." The NSA denied this allegation. In a statement on Tumblr, Director of National Intelligence James Clapper said this is "inaccurate and misleading information" about US intelligence. "The allegation that the National Security Agency collected more than 70 million 'recordings of French citizens' telephone data' is false." It seems to be a semantic discussion on the term "collecting" data.

Ending of privacy as a goal— it doesn't come as a shock for everyone. When asked about NSA hacking China, a spokeswoman of Ministry of Foreign Affairs of the People's Republic of China said that "China strongly advocates cyber security," implying that China is doing exactly the same. The Chief of the NSA, Keith Alexander, justified the PRISM program by saying that since the 9/11 attacks 50 terrorist attacks have been prevented in more than 20 countries. For example a planned bomb in the New York subway system was prevented because of the interception of an email sent to an address associated to Al Qaeda. Other plans for attack that were interrupted were the New York Stock Exchange and a Danish newspaper that published cartoons about the prophet Mohammed.



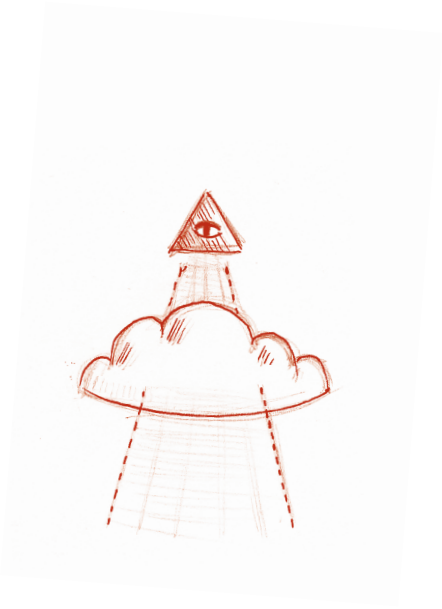
A poll of US Citizens that was held a few days after the Prism publications indicated the majority of the public supports the project. Two-thirds of US citizens approve on analyzing third party internet data by the government. On the collection of phone data, people are less supportive: 51% says Obama was right tapping into the phone conversations. Neelie Kroes, European Commissioner for Digital Affairs, stated the problem quite differently:

"If European cloud customers cannot trust the United States government, then maybe they won't trust US cloud providers either. If I am right, there are multibillion euro consequences for American companies. If I were an American cloud provider, I would be quite frustrated with my government right now."

And German Interior Minister Hans-Peter Friedrich called for a boycott of U.S. companies, declaring, "Whoever fears their communication is being intercepted in any way should use services that don't go through American servers."

THE IMPACT ON CLOUD COMPUTING

A greater understanding of this surveillance picture could have a deterring effect on all hosting and outsourcing services (not just cloud computing) in many countries. That's what Forrester analyst James Staten writes in his blog post. He thinks the true impact of PRISM and other surveillance programs could be as high as $180 billion. That would be a 25 percent hit on all U.S.-based IT service provider revenues through 2016.



The Information Technology & Innovation Foundation (ITIF) estimates did their own investigation. In their report "How much will Prism cost the US Computing Industry?" the ITIF claims that it seemed reasonable to suggest that US cloud businesses could lose between 10% and 20% of the overseas market to rivals. Author of the report, Daniel Castro, says the effect has already been felt. The ITIF survey found that of those outside the US, 10% had cancelled a project with a US-based cloud computing provider, and 56% would be "less likely" to use a US-based cloud computing service. Of those surveyed inside the US, 36% said that the NSA leaks had "made it more difficult" for them to do business outside the US.

Perhaps we should be a little skeptical of both ITIF and Forrester's estimates. U.S. cloud businesses may not take as bad of a hit. Concerns about government tracking are worldwide.

An interesting question was raised by a journalist of Venture Beat in his article "If NSA spying costs U.S. cloud companies $35B, where will that money go? China?" In this article Brian Jacobs is quoted. Jacobs is a partner of one of the major technology investment funds, Emerging Capital Partners (funded Salesforce and Yammer, for instance). Jacobs isn't that afraid of losing cloud deals to other countries because people trust the US government more than many other countries.

"While we are not universally liked around the world, most people understand that we have a high degree of transparency and due process compared to other governments, and we try not to arrest innocent people due to their beliefs, sexual preference, religion, etc. It would not surprise me if many foreign Internet users suspect their governments are snooping on their Internet traffic, whether they use U.S. services or local ones."

But Scott Fletcher, CEO of the UK based Ans Group, a Cloud provider, said that his business is going better because people know that they don't have any relationship with the government, unlike Google and Amazon. Staying far from government interference is the best practice for Cloud growth. But how to realize that is the big issue. In Germany four companies worked together and launched "E-mail made in Germany," offering data encryption and guaranteeing that the data will not pass the German border.

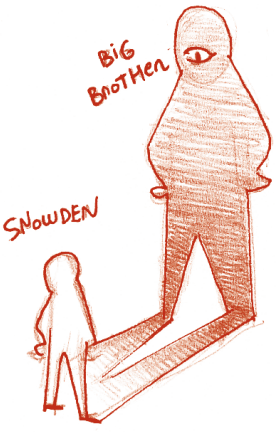
"While we are not universally liked around the world, most people understand that we have a high degree of transparency and due process compared to other governments... "

Meanwhile, Microsoft and Google press lawsuits agains the US government for the right to release more surveillance data. They feel they should have the right under the U.S. Constitution to specifically detail which information is being handed over upon the government's request--not just the total numbers.

Brad Smith, Microsoft's general counsel, said they will move forward with litigation in the hope that the courts will uphold their right to speak more freely. His hope is, while the discussion in parliament is growing, Congress will continue to press for the right of technology companies to disclose relevant information in an appropriate way. Whatever comes out of this lawsuit, Google and Microsoft will likely win the hearts of the people. And if they win, it's likely more secrets will be revealed.

FINAL THOUGHTS ABOUT OUR BIG BROTHERS

If the analysis done by the Guardian is right, the secret agencies are building machines with the explicit goal "to end privacy," which means being able to know everything about everybody. If so, is there anything what we can do about that? Whistleblowers and leakers, tweeters and facebook activist and secret agencies in a way are doing the same thing, making private stuff less private. Against every Big Brother are many little brothers like Edward Snowden. Even in China we now see the effects of social media on corruption and other misuse of power. Transparency and revealing the secrets of secret agencies and government officials is a way to organize checks and balances. You can argue whether that's good or bad, or question whether Snowden and other whistleblowers (before and after Snowden) are traitors or heros, but it's very unlikely that it will stop. In this rat race against secrecies, extreme transparency will be the direction society is heading to. Whistleblowers, wikileaks, Anonymous and other hacktivist are as much part of the culture as the secret agencies and the James Bonds. That's raising new questions for organizations, who "just want to do business" and are confronted with these issues when they offer cloud services. It raises questions for society as a whole. How will democracy look like in 2030? How will you and I deal with the fact that knowing something turns into knowing everything there is to know? How it is to live in this world of extreme transparency with no privacy at all is one of the biggest questions of this era.



Menno van Doorn
Director of VINT