EU Mission to the U.S. - JHA / HR / Political Counselors meeting - 10 June 2013 – A.M. Arnbak, LL.M.

PRISM: 'Obscured by Clouds or the Dark Side of the Moon?[1]

How to Address Governmental Access to Cloud Data from Abroad

*** * ***

Thank you very much for the invitation. I am very happy to speak here before you today in Washington D.C. I will talk about about our research in the context of the topical academic and policy conversation about the safeguarding of privacy, data security and confidentiality in the midst of the rapid transition of computing towards the cloud.

Whether or not one regards academia as a dry profession, we may let the creative juices flow when cooking up names for papers. About four months ago, we thought we were really on to something with Pink Floyd's album title 'Obscured by Clouds'. As the headlines keep on coming about speed of light intelligence analytics directly at the servers of 9 major U.S. internet companies, and then something with a Prism, we actually might have opted for 'Dark Side of the Moon' instead.

Today, I want to first elaborate on the legal reality of transnational surveillance in the cloud and the U.S. Foreign Intelligence Surveillance Act in particular, then say something about the apparent factual reality of PRISM, and ultimately look at what can be done on the regulatory and policy level.

Together with my colleagues dr. Joris van Hoboken and Prof. Nico van Eijk, I have conducted two studies into the legal possibilities in the U.S. legal framework for broad and unrestricted transnational surveillance. Our initial study led to global media coverage upon publication,[2] and we have decided to post the workshopped draft of our follow-up study online today. You are only the third audience to which we present our findings – questions, critique and relentless praise are more than appreciated!

Clearly, everyone is confronted every second of the day with the cloud transition. Privacy and cybersecurity are surely among the concerns. There are some difficult questions to be answered in this regard. I look forward to addressing some of them, and one of them in particular, namely the vulnerability of data in the cloud to access by governments abroad. Surveillance by one country, within one country, of foreign data is not new per se, but the cloud has served as a catalyst for an unprecedented rise in access to valuable governmental, corporate and personal information to spy on. We have researched transnational surveillance, by which we mean intelligence gathering by U.S. Authorities of non-US persons, businesses and governments within the U.S. without any transparency and accountability safeguards for those non-US entities. We find that a transition to the cloud leads to a decrease in overview and control over governmental

1 Van Hoboken, Joris V. J., Arnbak, Axel and Van Eijk, Nico, Obscured by Clouds or How to Address Governmental Access to Cloud Data from Abroad (May 30, 2013). Available at SSRN: http://ssrn.com/abstract=2276103

2 See for example: http://www.cbsnews.com/8301-205_162-57556674/patriot-act-can-obtain-data-in-europe-researchers-say/

access to data for law enforcement and national security purposes for any cloud customer. Transnational surveillance, we find, is obscured by clouds.

While our research could only point at the legal reality at access possibilities under the Foreign Intelligence Surveillance Act, notably its section 702 and art. 1881a, recent leaks surrounding the PRISM surveillance program conducted by the National Security Agency seems to prove our point.

President Obama and the Director of National Intelligence, mr. James Clapper, have referred to this section as the legal basis for the PRISM. I would like to stress here today that it is absolutely critical to get the facts right. While the PRISM program may seem as a the epic scandal that will define electronic communications environment, several critical facets remain unresolved. Did the National Security Agency install equipment at companies like Google, Facebook, Microsoft, Apple, etc. to acquire direct access to servers? It seems the case.[3] Did the NSA have direct access to all the customer data stored at these companies, or did it run sophisticated algorithms on real-time communications, through which certain data of interests could be filtered before sending a (and probably still substantial) part of the cloud data to the NSA for further analysis? Or did the NSA have a distant search engine capability in place? Not sure. Here lies an important task for the EU and its member states' missions, to which I will return later.

Ladies and Gentlemen, so what? The problem with governmental access from abroad can be illustrated with two examples. Within Europe, there has been rightfully been concern about the proper safeguarding of privacy of in the context of data retention for electronic communications data. This legislation mandates storage of location and traffic data of all European citizens, similar to the first leak in the now dubbed #NSAfiles related to metadata of Verizon customers. While there is disagreement of whether this data should be stored like this in the first place, we will all be able to agree that preventing unauthorized access to such data is extremely important. Now consider that the companies holding the communications metadata want to enter into the cloud? Does this mean that such data could become available to foreign governments for national security purposes without proper safeguards? Unfortunately, under the FISA, the answer to this question is yes.

Let’s think of another example. Consider the transition into the cloud of any given Ministry of Foreign Affairs. At stake is the confidentiality of diplomatic and foreign affairs data, clearly something not to make accessible to foreign governments. Should your Government be worried about which cloud provider to select in view of this concern? Again, the answer is yes, since – depending on the cloud provider – the data may become available to foreign governments abroad.

Notably, this is not a security issue in the technical sense. This is an issue of 'lawful access' in third countries, in the example of the United States, expressly authorized

3 See: http://www.guardian.co.uk/world/2013/jun/08/nsa-prism-server-collection-facebook-google

through the democratic process. The PRISM revelations have only confirmed what is possible and 'legal' under FISA; it is a legal enabler of global mass surveillance. Not only of consumers, but of corporations, media, non-governmental organizations and bureaucracies alike.

Now, can this current legal reality be resolved through regulation and other policies? This is the second research question in this second paper of ours. After a period of shying away from the issue, the issue of transnational surveillance governmental access to data from abroad is slowly but surely being raised – and after the PRISM leaks, one would expect also being taken up at the EU and national level. Although popular discussions remain somewhat ill-informed, a more nuanced discussion of the issues is starting to emerge.

In our research we discern and discuss four approaches: i) the possibility of limiting surveillance in the U.S. itself; ii) international law as a framework to impose some limitations; iii) the EU General Data Protection Regulation proposals and the EU Cloud Strategy, and iv) improved oversight on transnational intelligence gathering, on the national level. I will briefly summarize our conclusions.

The recent Supreme Court case Clapper v. Amnesty and the political climate here in Washington D.C. make it both legally and politically inconceivable that the U.S. legislature will amend FISA. The recent leaks might alter the political dimension of this, but you will probably be in a better position to reflect on that than me. In Europe, most of the attention is directed at possible amendment of the data protection framework. Of all the suggested proposals, the MEP In ‘t Veld amendments about data transfers and cloud computing are the most ambitious. They would introduce interesting new transparency obligations towards cloud customers and restrictions on bulk access such as the acquisitions made possible by the FISA in the U.S. But data protection as an avenue has its inherent legal limitations, particularly the fact that only a subset of cloud data actually constitutes personal data within the definition of the Data Protection Directive – and the currently negotiated Regulation appears to further limit that definition. It would make more sense to address these issues within the EU Cloud Communication, to the extent that this is possible under the EU Treaty that clearly excludes national security of its material scope – but of course not the protection of EU citizens against third countries. More on that a bit later.

The international law perspective on the matter of transnational surveillance needs more nuance than the notion that PRISM-like surveillance is an infringement of international human rights and national sovereignty in and by itself. The requests for access take place on the territory of the country claiming transnational intelligence jurisdiction. While the intrusion of law enforcement or intelligence agencies into computers on foreign territory does entail the extraterritorial use of power, transnational surveillance, that is access on the national level through internationally operating cloud or communications services, may not be an infringement of international law. The international human rights framework and the ECHR could, however, be valuable in the relation of citizens with their

own government that would fail to protect critical personal data infrastructure from governmental access abroad.

Not the easiest, but probably the most sensible way to address the issue would be through the application and possible strengthening of oversight over intelligence agency operations. Strengthening oversight could start at the national level through application of existing legal powers. The possibility of transnational surveillance could be addressed by national legislatures, for instance by requiring that, let's say, Dutch agencies should not be able to profit from information obtained about Dutch citizens from abroad without appropriate legal safeguards. In all of this, it should also be kept in mind that national intelligence agencies themselves have very good reasons to be worried about and investigate the possibility of access by foreign governments abroad.

Finally, I wanted to make some remarks about internet freedom. Ironically, while the U.S. Internet Freedom Agenda calls for unrestricted access of U.S. services to foreign markets, laws like FISA ensure that such access comes together with the possibility of mass surveillance of the respective populations. This may certainly not be the goal of the State Department’s focus on Internet Freedom. But until restrictions have been passed for intelligence gathering of non-U.S. citizens in views of the civil liberties outside U.S. borders, there is room for serious criticism of the 'internet freedom' that American Internet companies bring.

Many of the underlying goals of this Internet Freedom agenda are clearly applaudable. Probably, many of those gathered here today have worked on the dossier, that since the PRISM leaks has suffered a severe blow to its credibility. Not only for the interest of your own communications and that of the citizens, organizations, corporations and governments that you represent, but also for some of the more abstract notions of privacy, freedom and democracy, it is time to find out what is exactly happening behind the myst of the cloud. Will governments, in particularly the allies of the U.S., demand transparency for the surveillance of all those non-US customers of Google, Facebook, Apple and Microsoft services? Let me reiterate, that it is vital that the facts about PRISM emerge, and to nurture the public debate on the appropriate level of transnational surveillance. On a personal note, I believe it is quite disgraceful to have to rely on people risking their lives to foster public debate on these critical matters.

Considering all the interests involved in the transition to the cloud, it will be hard but must be possible to come to some agreement about restrictions on transnational intelligence gathering. If this remains obscured by the cloud, the economic, social and the democratizing promise that the electronic communications environment has already brought will halt with the speed of light in this Prism of distrust and surveillance. Now, on the dark side of the moon, who said this profession was dry? Thank you for your attention.