# The coming data wars, the rise of digital totalitarianism and why internet users need to take a stand

You may have read my last post [1], a few days ago, on why I think the PRISM / Snowden / NSA affair is a game changer for the future of the Internet. It looks like a good many people agreed with my 'analysis' considering the number of tweets, comments and FB-likes (and phone calls:) that the post received; but then again there seems to be little concern voiced on the consequences of these events, in the media, so far. Generally, people seem concerned but not appalled or even really worried – see the chart below (which is US-only so… not surprised to see that, really). What gives? Are we so hooked on social media, cloud computing and free online services and platforms that we would agree to anything to keep them going?

I thought I should fuel the fire a bit more and share some further thoughts on what I think is happening with so called Big Data and 'Publicy', so here it goes.

As you may know, I have riffed on the 'Data is the new Oil' theme [2] for the past 3-4 years and confess to be guilty of some serious meme-laundering:). However, as we can see right now, data is indeed well on the way of replacing oil is the primary driver of our economies, on a global scale. Here's why, how – and what it means:

1) We – the people formerly known as consumers – have struck many more or less 'faustian bargains' with the likes of Google, Facebook, QQ, Twitter, Xing, LinkedIn etc to use their cool and often quite addictive platforms and gardens in exchange for allowing access to our user data and digital footprints freely, widely and openly. We have received pretty good value for doing this deal, so far, I think, and these new kinda-sorta Exxon-Mobil-like companies [3] have prospered handsomely: they got plenty of (data)-oil, they mined it, refined it and used it to fuel an increasing number of shiny new digital vehicles (i.e. brands, marketers and advertisers). So far so good.

2) Most of these companies are based in the USA where they are subject to a seemingly mushrooming number of laws that by many accounts have been moving the country – and some of its allies – towards a digital surveillance society. Some people such as Jakob Augstein from the German magazine 'Der Spiegel' even called this a U.S. move towards 'soft totalitarianism' [4]; to me this seems merely the logical extension of the paranoid U.S. strategy that was put into place after 9/11 and the subsequent Patriot-act-fueled expansions of government agency powers under the pretense of national security.

As such, many of these companies – i.e. those we have placed our trust i.e. personal data in – are now facing a real and potentially deadly dilemma as they cannot seem to warrant our data's safety and our most basic civil rights any longer. Yes, sure, we have always known that this is possible and even likely to be the case, but the scope and sheer volume of the data-hoovering [5] undertaken by the authorities that is coming to light at this point is like the difference between a puddle and an ocean. And the issue is NOT whether we have something to hide – it's whether we have a say about it.

3) Governments around the world are getting smart to the principles and juicy possibilities of Big Data [6], i.e. primarily the fact that individual data points may not mean much, by themselves, but in huge and complete aggregation they become tremendously powerful. Imagine sucking in i.e. 'hoovering' the metadata of your phone calls (i.e. who you call, when, how long etc), your most prominent keywords in your email inbox, your public Facebook / LinkedIn / Twitter feeds, your browsing history, your mobile phone location data and much more (yes, think tax records and credit card data, and how often you cross which toll-bridge) and putting it through a smart software engine that spits out who you are and what are you likely to do / think / vote / buy – like Klout or Peerindex [7]or GoogleNow but on the best amphetamines that money/data can buy. And then, cross-reference them with 100s of your friends and contacts. Now, this is an altogether different game. Then, imagine what anticipatory platforms – basically prediction engines [8]- such as GoogleNow or Siri could do if they had all that data about you… you get my drift.

This is not the deal most of us signed up for. Or is it? (please comment below!!)

Of course, the tantalizing prospect of having the entire population's data sliced and diced at will; of almost every single citizen being digitally naked is understandably irresistible to any law enforcement official – hey, if marketing people and brands can segment and target their individual followers online to sell them stuff they don't need, why shouldn't government agencies be able to do some simple observing?

*Bottom line: the very same data oil that to a very large extend already fuels the $600 Billion advertising industry will fuel something in the neighborhood of a $1 Trillion global data monitoring and surveillance business – and it's you and me that will make this happen by allowing them to drill into our data i.e. into us.*

Now, here is where it gets interesting: as you may have noticed, we have many armed conflicts and wars over oil (think Iraq – this war was not about WMDs but about fears over oil supply, and regional power structures), and now that the oil economy is invariably winding down in the next decade because of rapid technological progress in wind, water, sun (WWS) and even

nuclear energy and t[9]he glaringly obvious need to reduce global warming [10], guess what is next: **DATA will become the #1 source of global conflicts, and yes, wars will be fought over it** – and Edward Snowden may well be the first casualty in this fight (and you have to admire him for knowingly stepping into this huge pile of s***).

So let me ask this simple question: in the case of oil, we have already experienced the consequences of a handful of corporations exploiting an essentially public i.e. common resource, and scoring enormous profits with it while governments subsidies of fuel exceed $ 1 Trillion per year, worldwide. Regardless of the fact the the planet and by extension all us, its inhabitants, really 'owned' the oil and gas that these enterprising corporations [11] took out, refined and sold back to us, none of us had any say about whether this is a good thing or not – and now all of us are paying the price of an increasingly toxic and overheating planet. Do we want the same thing to happen with 'the next oil' i.e. data? Do we really want to tacitly sanction the use of our data streams (those new fossil fuel-makers) from what will soon be 3-5 Billion people i.e. 'sources' so that the new Exxon-Mobil's of the world can drill and refine it and sell it back to us, without any control or redress or other kind of real power, in return?

If data is indeed a new kind of public resource (consider the 100s of open data initiatives by cities and governments around the world) than we need to have collective authority over it, not leave our fate to some large corporations or, worse, the national governments that regulate them under their own secret agendas where we have no redress or opt-in whatsoever.

**Google, Facebook, Twitter, Apple, MSFT, hear the call: unless you fix these issues and significantly step up your efforts to defend the rights of your users you may very soon need to *pay them* to use your services. We trusted you and now it's time to act on our behalf.**

In my view, it is indeed totally unacceptable that the U.S. government and its law enforcement agencies, and by extension its various allies around the globe, or some secret FISA court [12] apparently get to define and enforce the global strategy on this 'data-oil'.

This is my information and the Internet is our show, not theirs – play the game right, or I'll stop playing. What about you?

PS: In the interest of full disclosure: I do some keynotes and talks for Google, sometimes.

Related:

SOCMINT activities [13] in the UK: "On June 26, *The Guardian* reported [14] that the very same unit had a "secret database" that had labelled some 9,000 individuals—many from political groups—as "domestic extremists." It adds to the growing number of questionable surveillance tactics used by the police. What is particularly troublesome is that these abuses occurred even with the apparent existence of proper legislation and oversight—something the snooping of social media data currently does not have…"

Nice and succinct: Der Spiegel [15]: "Friedrich's quote from the weekend was particularly quaint: "I have no reason to doubt that the US respects rights and the law." Yet in a way, he is right. The problem is not the violation of certain laws. Rather, in the US the laws themselves are the problem. The NSA, in fact, didn't even overreach its own authority when it sucked up 97 billion pieces of data in one single 30-day period last March. Rather, it was acting on the orders of the entire US government, including the executive, legislative and judicial branches, the Democrats, the Republicans, the House of Representatives, the Senate and the Supreme Court. They are all in favor. Democratic Senator Dianne Feinstein, chair of the Senate Intelligence Committee, merely shrugged her shoulders and said: "It's legal."

**A Monitored Human Being Is Not a Free One**

What, exactly, is the purpose of the National Security Agency? Security, as its name might suggest? No matter in what system or to what purpose: A monitored human being is not a free human being. And every state that systematically contravenes human rights, even in the alleged service of security, is acting criminally.

The brilliant-as-usual Guardian [16]: "Prism: secret surveillance could destroy democracy rather than defend it. Don't fall for the narrative that if you've nothing to hide, you needn't worry. Our privacy is not a luxury. Privacy is a fundamental human right which is essential if we wish to live in dignity and security. It cannot be forfeited so easily. Private companies and states alike must be more cautious in using our data and avoiding any abuse that could arise from indiscriminately mining them. Spying on individuals on a massive scale, without strict legal rules and democratic oversight, can have adverse effects on freedom of speech, association and participation, and can create a nefarious social climate where all individuals are seen as potential suspects. States, of course, have a duty to ensure security within their borders, and in doing so they can undertake the secret surveillance of individuals who can pose a threat. But those who implement secret surveillance risk undermining or even destroying democracy while pretending to defend it. To stem this risk, states and private companies must develop surveillance and data collection policies that respect human rights. First, the law must be precise and clear as to the offences, activities and people subjected to surveillance, and must set out strict limits on its duration, as well as rules on disclosure and destruction of surveillance data. Second, rigorous procedures should be in place to order the examination, use and storage of the data obtained, and those subjected to surveillance should be given a chance to exercise their right to an effective remedy. Third, the bodies supervising the use of surveillance should be independent and appointed by, and accountable to, parliament rather than the executive"

Couldn't have said it better myself:)

1. http://futuristgerd.com/2013/06/22/5-reasons-why-the-snowden-nsa-prism-affair-is-a-game-changer-for-the-future-of-the-internet/
2. http://gerd.fm/datanewoil
3. http://www.salon.com/2013/05/06/facebook_and_google_are_the_new_exxon/
4. http://www.spiegel.de/international/world/europe-must-stand-up-to-american-cyber-snooping-a-906250.html
5. http://www.theatlanticwire.com/technology/2013/06/heres-almost-whole-truth-about-how-prism-works/66272/
6. http://gerd.fm/bigdatagerd
7. http://www.peerindex.com/gleonhard
8. http://www.technologyreview.com/news/514366/with-personal-data-predictive-apps-stay-a-step-ahead/
9. http://futuristgerd.com/wp-content/uploads/2013/06/earth-burning-tripping-oil.jpg
10. http://www.greenfuturist.com/tagged/climate%20change
11. http://www.forbes.com/pictures/eglg45fhihl/not-just-the-usual-suspects-3/
12. http://www.politico.com/story/2013/06/microsoft-fisa-petition-nsa-prism-93475.html?hp=l9
13. http://arstechnica.com/tech-policy/2013/06/meet-prisms-little-brother-socmint/
14. http://www.guardian.co.uk/uk/2013/jun/25/undercover-police-domestic-extremism-unit
15. http://www.spiegel.de/international/world/europe-must-stand-up-to-american-cyber-snooping-a-906250.html
16. http://www.guardian.co.uk/commentisfree/2013/jun/26/prism-surveillance-could-destroy-democracy