http://www.faz.net/aktuell/feuilleton/debatten/ueberwachung/information-consumerism-the-price-of-hypocrisy-12292374.html

Information Consumerism The Price of Hypocrisy

24.07.2013 · Even the best laws will not lead to a safer internet. We need a sharper picture of the information apocalypse that awaits us in a world where personal data is traded to avert the catastrophy.

Von Evgeny Morozov

Dr. Jekyll and Mister Hyde? The military and the IT sphere already affiliated, as you may see in the person of one of the most powerful men of the world: Keith Alexander, Director of the NSA, recruiting hackers at Defcon 2012, wearing a t-shirt of the civil rights organisation „Electronic Frontier Foundation"; in service uniform on the right

The problem with the sick, obsessive superpower revealed to us by Edward Snowden is that it cannot bring itself to utter the one line it absolutely must utter before it can move on: "My name is America and I'm a dataholic." For American spies, Big Data is like crack cocaine: just a few doses – and you can forget about mending your way and kicking the habit. Yes, there's an initial illusion of grandeur and narcissistic omnipotence – just look at us, we could prevent another 9/11! – but a clearer, unmediated brain would surely notice that one's judgment has been severely impaired. Prevent another 9/11? When two kids with extensive presence on social media can blow up a marathon in Boston? Really? All this data, all this sacrifice– and for what?

So let us not pass over America's surveillance addiction in silence. It is real; it has consequences; and the world would do itself a service by sending America to a Big Data rehab. But there's more to learn from the Snowden affair. *It has also busted* a number of myths that are only peripherally related to surveillance: myths about the supposed benefits of decentralized and commercially-operated digital infrastructure, about the current state of technologically-mediated geopolitics, about the existence of a separate realm known as "cyberspace." We must take stock of where we are and reflect on where we soon will be, especially if we fail to confront – legally but, even more importantly, intellectually – the many temptations of information consumerism.

Why surrender control over electronic communications?

First of all, many Europeans are finally grasping, to their great dismay, that the word "cloud" in "cloud computing" is just a euphemism for "some dark bunker in Idaho or Utah." Borges, had he lived long enough, would certainly choose a server rack – not a library – as the primary site for his surreal stories. A database larger than the world it is meant to represent: a Borges short story or a slide from an NSA PowerPoint? One can't say for sure.

Second, ideas that once looked silly suddenly look wise. Just a few months ago, it was customary to make fun of Iranians, Russians and Chinese who, with their automatic distrust of all things American, spoke the bizarre language of "information sovereignty." What, the Iranians want to build their own national email system to lessen their dependence on Silicon Valley? That prospect seemed both futile and wrong-headed to many Europeans: what a silly waste of resources! How could it possibly compete with Gmail, with its trendy video chats and slick design? Haven't Europeans tried – and failed – to launch their own search engine? Building airplanes that can compete with Boeing is one thing – but an email system? Now, that's something Europe – let alone Iran! – would never be able to pull off.

Look who's laughing now: Iran's national email system launched a few weeks ago. Granted the Iranians want their own national email system, in part, so that they can shut it down during protests and spy on their own people AT other times. Still, they got the geopolitics exactly right: over-reliance on foreign communications infrastructure is no way to boost one's sovereignty. If you wouldn't want another nation to run your postal system, why surrender control over electronic communications?

The public-private partnership of American infrastructure

Third, the sense of unconditional victory that civil society in both Europe and America felt over the defeat of the Total Information Awareness program – a much earlier effort to establish comprehensive surveillance – was premature. The problem with Total Information Awareness was that it was too big, too flashy, too dependent on government bureaucracy. What we got instead, a decade later, is a much nimbler, leaner, more decentralized system, run by the private sector and enabled by a social contract between Silicon Valley and Washington: while Silicon Valley runs, updates and monetizes the digital infrastructure, the NSA can tap IT on demand. Everyone specializes and everyone wins.

This is today's America in full splendor: what cannot be accomplished through controversial legislation will be accomplished through privatization, only with far less oversight and public control. From privately-run healthcare providers to privately-run prisons to privately-run militias dispatched to war zones, this is the public-private partnership model on which much of American infrastructure operates these days. Communications is no exception. Decentralization is liberating only if there's no powerful actor that can rip off the benefits after the network has been put in place. If such an actor exists – like NSA in this case – decentralization is a mere shibboleth. Those in power get more of what they want quicker – and pay less for the privilege.

A noble mission and awful trip-planning skills

Fourth, the idea that digitization has ushered in a new world, where the good old rules of realpolitik no longer apply, has proved to be bunk. There's no separate realm that gives rise to a new brand of "digital" power; it's one world, one power, with America at the helm. Google's CEO Eric Schmidt and Jared Cohen, a former senior official at the State Department who went to work for Google, had the misfortune to publish a book that assured us that this was no longer the case – "The New Digital Age" – just a few months before the Snowden revelations. Rare is a book that ages so quickly. Look no further than "Internet asylum seekers" in its index. "A dissident who can't live freely under an autocratic Internet and is refused access to other states' Internets will choose to seek physical asylum in another country to gain virtual freedom on its Internet," they claim. "Being granted virtual asylum could be a significant first step toward physical asylum, a sign of trust without the full commitment."


© Reuters
Edward Snowden auf dem Moskauer Flughafen Scheremetjewo

The sheer naivete of statements like this – predicated on the assumption that somehow one can "live" online the way one lives in the physical world and that virtual politics works on a logic different from regular politics – is illustrated by the sad case of Edward Snowden, a man with a noble mission and awful trip-planning skills. If it's "virtual asylum" that Snowden is after, he can get his dose of "virtual

freedom" in Sheremetyevo airport in Moscow. Somehow – silly him? – "virtual freedom" doesn't seem to be enough and it hasn't occurred to him – perhaps, he has not read the book yet? – to seek "virtual asylum." Bolivia's Evo Morales, stranded in Austria on suspicion that his plane had been carrying Snowden, would have had a good laugh had he stumbled upon "The New Digital Age" in a Vienna airport bookstore. Perhaps, had Moralez only tweeted harder, none of this would have happened.

Security and privacy on the level of the telephone network

Fifth, the once powerful myth that there exists a separate, virtual space where one can have more privacy and independence from social and political institutions is dead. To see why, look no further than the Microsoft memo issued after The Guardian had reported that NSA may have been tapping Skype chats and video calls (Skype is now owned by Microsoft). Buried in Microsoft's non-denial is a very peculiar line. Justifying the need to make its digital products compatible with the needs of security agencies, Microsoft's general counsel wrote that "looking forward, as Internet-based voice and video communications increase, it is clear that governments will have an interest in using (or establishing) legal powers to secure access to this kind of content to investigate crimes or tackle terrorism. *We therefore assume that all calls, whether over the Internet or by fixed line or mobile phone, will offer similar levels of privacy and security*." Read this again: here's a senior Microsoft executive arguing that making new forms of communication less secure is inevitable – and probably a good thing.
For most of the 1990s, everyone thought that digitization would usher in the so-called "convergence": undoubtedly, a good thing as far as security was concerned. Thus, the reasoning went, as they move to one single network, old forms of communication – the good-old telephone and the like – would eventually become as secure as encrypted email. But we have actually moved in the opposite direction. What we have now is one single network – that much we got right – but the one where security and privacy have returned to the level of the telephone network. It's the telephone – not encrypted email – that is our common denominator at least when it comes to wiretapping potential. Convergence did happen – we weren't fooled! – but, miraculously, technologies converged on the least secure and most wiretap-friendly option available.

The users in authoritarian states will suffer the most

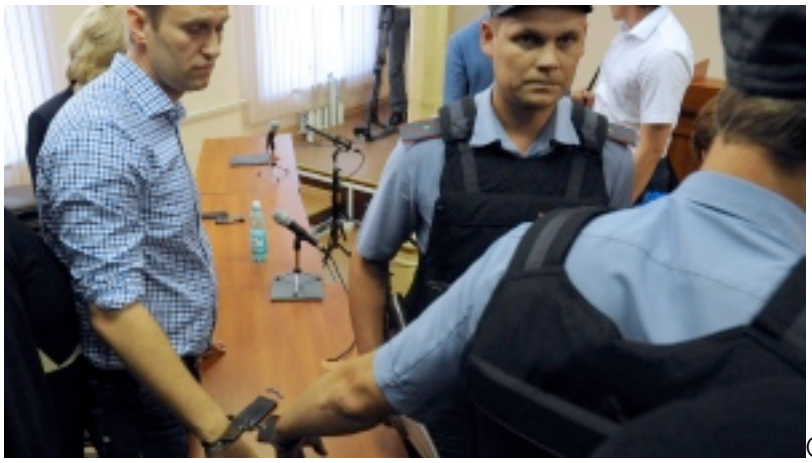
This has disastrous implications for anyone living in dictatorships. Once Microsoft and its peers start building software that is insecure by design, it turbocharges the already comprehensive spying schemes of authoritarian governments. What neither NSA nor elected officials seem to grasp is that, on matters of digital infrastructure, domestic policy is also foreign policy; it's futile to address them in isolation. So, we want to catch all the terrorists before they are born? Fine, Big Data – and big bugs in our software and hardware – are here to help. But, lest we forget, they would also help the governments of China and Iran to predict and catch future dissidents. We can't be building insecure communication infrastructure and expect that only Western governments would profit from it.

This brings us to the most problematic consequence of Snowden's revelations. As bad as the situation is for Europeans, it's the users in authoritarian states who will suffer the most. And not from American surveillance, but from domestic censorship. How so? The already mentioned push towards "information sovereignty" by Russia, China or Iran would involve much more than protecting their citizens from American surveillance. It would also trigger an aggressive push to shift public communication among these citizens – which, to a large extent, still happens on Facebook and Twitter – to domestic equivalents of such services.

Instead of blaming Snowden, Washington must thank him

Authoritarian governments have good reasons to fear Twitter and Facebook, over which they exercise far less control. It's probably not a coincidence that LiveJournal, Russia's favorite platform, suddenly had maintenance issues – and was thus unavailable for general use – at the very same time that a Russian court announced its verdict to the popular blogger-activist Alexei Navalny. For all the concerns about Americanization and surveillance, US-based services like Facebook or Twitter still offer better protection for freedom of expression than their Russian, Chinese or Iranian counterparts. The latter censor more and, as the LiveJournal example shows – LiveJournal belongs to a Russian oligarch – they can go offline at politically convenient times. If, as a political dissident, you had to

choose between organizing your protest on Facebook or Vkontakte, Facebook's Russian equivalent, you'd be far better off doing it on Facebook. Governments of less democratic regimes will surely explore the anti-US populism generated by Snowden revelations to leave protesters just one – domestic – option.

 © dpa

Nach dem Urteil: Der russiche Blogger Aleksej Nawalnyi wird in Handschellen abgeführt

This is the real tragedy of America's "Internet freedom agenda": it's going to be the dissidents in China and Iran who will pay for the hypocrisy that drove it from the very beginning. America has managed to advance its communications-related interests by claiming high moral ground and using ambiguous terms like "Internet freedom" to hide many profound contradictions in its own policies. On matters of "Internet freedom" – democracy promotion rebranded under a sexier name – American enjoyed some legitimacy as it claimed that it didn't engage in the kinds of surveillance that it itself condemned in China or Iran. Likewise, on matters of cyberattacks, it could go after China's cyber-espionage or Iran's cyber-attacks because it assured the world that it engaged in neither.

Both statements were demonstrably false but lack of specific evidence has allowed America to buy some time and influence. These days are gone. Today, the rhetoric of "Internet freedom agenda" looks as trustworthy as George Bush's "freedom agenda" after Abu Ghraib. Washington will have to rebuild its policies from scratch. But, instead of blaming Snowden, Washington must thank him. He only exposed the shaky foundations of already unsustainable policies. These policies, built around vaporous and ambiguous terms like "Internet freedom" and "cyberwar" would have never survived the complexities of global politics anyway.

All objects and appliances turn "smart" and get connected

What is to be done? Let's start with surveillance. So far, most European politicians have reached for the low-hanging fruit – law – thinking that if only they can better regulate American companies – for example, by forcing them to disclose how much data and when they share with NSA – this problem will go away. This is a rather short-sighted, naïve view that reduces a gigantic philosophical problem – the future of privacy – to seemingly manageable size of data retention directives. If only things were that simple! Our current predicaments start at the level of ideology, not bad policies or their poor implementation. This is not to oppose more regulation of technology companies – Europe should have done this a decade ago instead of getting caught in the heady rhetoric of "cloud computing" – but only to point out that the task ahead is far more intellectually demanding.

Assume, for a moment, that Europe forces all the laws it wants on US technology companies. It's a very unlikely hypothetical – not with their growing lobbying power in Brussels– but let's forget this for a moment. What will happen in five years, as all objects and appliances turn "smart" – i.e. they suddenly have a cheap but sophisticated sensor built into them – and become connected to each other and to the Internet? Many such objects are already commercially available and many more will be soon: smart forks that monitor how fast we eat; smart toothbrushes that monitor how often we brush our teeth; smart shoes that tell us when they are about to get worn out; smart umbrellas that go online

to check when it will rain and warn us to take them with us on leaving the house. And then, of course, there's that smartphone dangling in your pocket and – soon – Google Glasses adoring your face. *(Hapilabs presenting a smart fork)*

All these objects are capable of generating a data trail. Collect information from several such objects, put it together and – functionally at least– you can generate the same inferences and predictions that NSA generates by watching our email communications or phone records. In other words, NSA can figure out where you are by monitoring your cellphone – or by getting data from your smart shoes or your smart umbrella. Likewise, they don't have to install a security camera in your kitchen to know what you've been eating: they can figure it out by tinkering with the smart toothbrush in your toothbrush or the smart trashbin in your kitchen. If we don't consider these new listening devices in our legal calculus, there's little point to build the world's most secuire email system or a mobile network: NSA will obtain data that allows them to continue their work through other, more creative means. They might even buy IT on the open market. Some dismiss such concerns, arguing that our email communication feels too private to be sold as if it were just another commodity. True. However, we are perfectly okay with having a Google algorithm scour through our email in order to show us an ad. It's this customized ad – based on automated on-the-fly analysis and classification – that allows to keep Google's sophisticated (and rather costly) email system free of charge. Note that it's this tacit agreement – that Google can use an algorithm to analyze our email communications and sell us the matching adds – that keeps our email communication both free and accessible to the NSA. Google could have easily chosen to encrypt our communications in a way that its own algorithms wouldn't be able to decipher, depriving both itself and the NSA of much-coveted data. But then Google wouldn't be able to offer us a free service. And who would be happy about this?

Laws won't be of much help

As our gadgets and previously analog objects become "smart," this Gmail model will spread everywhere. One set of business models will supply us with gadgets and objects that will either be free or be priced at a fraction of their real cost. In other words, you get your smart toothbrush for free – but, in exchange, you allow it to collect data on how you use the toothbrush. It's this data that will eventually finance the cost of the toothbrush. Or, for objects with screens or speakers, you might see or hear a personalized ad based on your use of the device – and it's the ad that will underwrite the cost. This, for example, is the model that Amazon is already pursuing with its Kindle ereaders: if you want a cheaper model, you simply accept to see advertising on their screens. Amazon's ultimate Faustian bargain would be to offer us a free ereader along with free and instantaneous access to all of the world's books on one condition: we will agree to let it analyze everything we read and serve us ads accordingly.

(A yawn rewarded with a coffee: Douwe Egberts is proud of its using facial recognition)
Under a slightly modified model – which is already available through various start-ups known as "personal data lockers" – you can actually make money off that data by selling it yourself – and not just from the toothbrush but from across any smart object that you interact with: your car, your desk, your trashbin. One start-up – Miinome – even allows you to make money by putting up your genetic code online; whenever a third-party company accesses it – perhaps, to customize advertising or to use it in some Big Data experiment – you get a small payment. Essentially, the ability to insert a sensor and an Internet connection into everything, including our body, makes it possible to commodify everything and to attach a price on the information generated in the context of its use. Sensors and ubiquitous connectivity help to create new, liquid markets in such information, allowing citizens to monetize self-surveillance.

If this is, indeed, the future that we are heading towards, it's obvious that laws won't be of much help, as citizens would voluntarily opt for such transactions – the way we already opt for free (but monitorable) email and cheaper (but advertising-funded) ereaders. Spies from the NSA will have two options: they can either go and ask data from companies that build all these smart objects – from smart shoes to smart toothbrushes – or they can buy it in the open market – as this data would eventually be traded – by us, citizens. In short, what is now collected through subpoenas and court orders could be collected entirely through commercial transactions alone.

Market logic has replaced morality

Policymakers who think that laws can stop this commodificaton of information are deluding themselves. Such commodification is not happening against the wishes of ordinary citizens but *because* this is what ordinary citizen-consumer want. Look no further than Google's email and Amazon's Kindle to see that no one is forced to use them: people do it willingly. Forget laws: it's only through political activism and a robust intellectual critique of the very ideology of "information consumerism" that underpins such aspirations that we would be able to avert the inevitable disaster.

Where could such critique begin? Consider what might, initially, seem like a bizarre parallel: climate change. For much of the 20th century, we assumed that our energy use was priced correctly and that it existed solely in the consumer paradigm of "I can use as much energy as I can pay for." Under that paradigm, there was no ethics attached to our energy use: market logic has replaced morality – which is precisely what has enabled fast rates of economic growth and the proliferation of consumer devices that have made our households electronic paradises free from tiresome household work. But as we have discovered in the last decade, such thinking rested on a powerful illusion that our energy use was priced correctly – that we in fact paid our fair share. (Carbon credits trading scheme was meant to rectify this problem – before it collapsed.)

You cannot imagine the information disaster that easily

But of course we had never priced our energy use correctly because we never factored in the possibility that life on Earth might end even if we balance all of our financial statements. So now your decision what car to drive or how much light to have in your living room is no longer a decision affected *solely* by your ability to pay for electricity; it's also an ethical decision that each of us makes for ourselves (apparently, not very effectively). The point is that, partly due to successful campaigns by the environmental movement, a set of purely rational, market-based decisions have suddenly acquired political latency, which has given us differently designed cars, lights that go off if no one is in the room, and so forth. It has also produced citizens who – at least in theory – are encouraged to think of implications that extend far beyond the ability to pay their electricity bill.

Now, this might seem like an odd parallel to draw to information sharing but it's actually not that outlandish. Right now, your decision to buy a smart toothbrush with a sensor in it – and then to sell the data that it generates – is presented to us as just a purely commercial decision that affects no one but us. But this is so only because we cannot imagine an information disaster as easily as we can imagine an environmental disaster. We have become very bad dystopians – and our technophilic intellectuals, in love with Silicon Valley and buzzwords like "innovation," are partly to blame. But that the disaster is slow and doesn't lend itself to vivid visualizations doesn't make it less of a disaster!

Political and moral consequences to information consumerism

What we need is a sharper, starker picture of the information apocalypse that awaits us in a world where personal data is traded like coffee or any other commodity. Take the oft-repeated argument about the benefits of trading one's data in exchange for some tangible commercial benefit. Say, for example, you install a sensor in your car to prove to your insurance company that you are driving much safer than the average driver that figures in their model for pricing insurance policies. Great: if you are better than the average, you get to pay less. But the problem with averages is that half of the population is always worse than the benchmark. Inevitably –regardless of whether they want to monitor themselves or not – that other half will be forced to pay more, for as the more successful of us take on self-tracking, most social institutions would (quite logically) assume that those who refuse to self-track have something to hide. Under this model, the implications of my decision to trade my personal data are no longer solely in the realm of markets and economics – they are also in the realm of ethics. If my decision to share my personal data for a quick buck makes someone else worse off and deprives them of opportunities, then I have an extra ethical factor to consider – economics alone doesn't suffice.
All of this is to say that there are profound political and moral consequences to information consumerism– and they are comparable to energy consumerism in scope and importance. Making these consequences more pronounced and vivid is where intellectuals and political parties ought to focus their efforts. We should do our best to suspend the seeming economic normalcy of information sharing.

An attitude of "just business!" will no longer suffice. Information sharing might have a vibrant market around it but it has no ethical framework to back it up. More than three decades ago, Michel Foucault was prescient to see that neoliberalism would turns us all into "entrepreneurs of the self" but *let's* not forget that entrepreneurship is not without its downsides: as most economic activities, it can generate negative externalities, from pollution to noise. Entrepreneurship focused on information sharing is no exception.

We need the mainstreaming of "digital" topics

European politicians can try imposing whatever laws they want but as long as the consumerist spirit runs supreme and people have no clear ethical explanation as to why they shouldn't benefit from trading off their data, the problem would persist. NSA surveillance, Big Brother, Prism: all of this is important stuff. But it's as important to focus on the bigger picture -- and in that bigger picture, what must be subjected to scrutiny is information consumerism itself – and not just the parts of the military-industrial complex responsible for surveillance. As long as we have no good explanation as to why a piece of data shouldn't be on the market, we should forget about protecting it from the NSA, for, even with tighter regulation, intelligence agencies would simply buy – on the open market – what today they secretly get from programs like Prism.

Some might say: If only we could have a digital party modeled on the Green Party but for all things digital. A greater mistake is harder to come by. It's wrong to think that all this digital stuff can just be pigeonholed and delegated to the bright young people who know how to code. This "digital stuff" is of fundamental importance for the future of privacy, autonomy, freedom, and democracy itself: these are matters that should be of importance to every political party. For a mainstream political party today to abandon responsibility over the "digital" is tantamount to abandoning responsibility over the future of democracy itself.

What we need is the mainstreaming of "digital" topics – not their ghettoization in the hands and agendas of the Pirate Parties or whoever will come to succeed them. We can no longer treat the "Internet" as just another domain – like, say, "the economy" or the "environment" – and hope that we can develop a set of competencies around it. Rather, we need more topical domains - "privacy" or "subjectivity" to overtake the domain of the network. Forget an ambiguous goal like "Internet freedom" – it's an illusion and it's not worth pursuing. What we must focus on is creating environments where actual freedom can still be nurtured and preserved.

A much more dangerous threat to democracy than the NSA

The Pirates's tragic miscalculation was trying to do too much: they wanted to change both the *process* of politics and its *content*. That project was so ambitious that it was doomed to failure from the very beginning. Besides, the political usefulness of changing the *process* – whether it was a push towards greater participation or more transparency over legislative meetings – should itself be in question; whatever reforms the Pirates have been advancing did not seem to stem from some long critical reflections of the pitfalls of the current political system but, rather, from their belief that the political system, incompatible with the most successful digital platforms from Wikipedia to Facebook, must be reshaped in their image. This was – and is – nonsense. A parliament is, in fact, different from Wikipedia – but the success of the latter tells us absolutely nothing about the viability of the Wikipedia model as a template for remodeling our political institutions (and let us not beat around the bush: they are far from perfect, these parliaments, as the financial crisis has indicated). But the good thing that did come out of the Pirates was the nudge to get everyone else thinking about digital matters and their impact on the future of democracy. This is the content – rather than the process – part. That project must continue but, perhaps, be reoriented from pursuing the faux goal of "Internet freedom" to thinking about preserving real freedoms instead.

In as much as the Snowden affair has forced us to confront these issues, it's been a good thing for democracy. Let's face it: most of us would rather not think about the ethical implications of smart toothbrushes or the hypocrisy involved in Western rhetoric towards Iran or the genuflection that more and more European leaders show in front of Silicon Valley and its awful, brain-damaging language, the Siliconese. The least we can do is to acknowledge that the crisis is much deeper and that it stems from

intellectual causes as much as from legal ones. Information consumerism, like its older sibling energy consumerism, is a much more dangerous threat to democracy than the NSA.