The Kontrollverlust of the Nation-State and the Rise of the Platforms

Michael Seemann

Essay – October 11, 2015

Michael Seemann argues that there are a lot of ways that governments and nation-states can lose control. First, they lose control over their data. This is neither a particularly new thing nor unique to the nation-state. The loss of control over one's data is an issue that affects everyone. But there is also another way that the nation-state loses control, Seemann asserts. The world is currently undergoing a transition that is driven by that first level of *Kontrollverlust*, which transfers much of the power and control from the nation-state to new players: the platforms. This essay belongs to *Culture of Control* [www.onlineopen.org/culture-of-control], a collaboration with Stroom Den Haag.

Since Wikileaks revealed large amounts of US intelligence to the public in 2010, most people are now more aware of the vulnerability of the nation-state: that it must keep it's secrets safe in order to function. (At least, this is what the nation-state believes.) But as technology evolves, it seems less and less able to do so.

This inability to control its own information is what I chose to call "*Kontrollverlust*" [www.onlineopen.org/digital-tailspin], which has emerged as a result of three major technological drivers.

1. The increased installation of sensors everywhere including in smartphones, CCTV cams, Internet, home automation, smart cities, intelligent sensors in thermostats, in cars, on game consoles, smartwatches, smart wear, etc. We daily increase our connections between the physical and digital worlds. There is no offline anymore. If you are part of the world, you are part of the Internet.
2. Increases in data storage and conduction capacities: The computer is more of a copier than a calculator. Most CPU operations basically consist of copying bits from A to B so that the Internet basically functions as a huge network of copy machines, copying data globally. When you realise that the capacities of the copy machines and their vast connections double every two years you begin to comprehend how easy it is to maintain and save data.
3. The increased capacities to make sense of these huge amounts of data: You may think that this much data simply cannot be managed. But you would be wrong. Big data, new pattern recognition technologies, deep learning algorithms and so on are evolving technologies as they develop increased capacities to find relevant data within the haystack and link it with in order to generate knowledge.

If you keep these three drivers in mind, you will begin to understand why it has become so difficult to keep secrets and to control distribution channels of intangible goods. There are many ways to lose control over your data and this becomes increasingly apparent every day. This is Kontrollverlust.

In a way, we are not that different from a nation-state as no one wants to see his or her

secrets revealed publicly, but we all have to deal with *Kontrollverlust*. But the main difference between the people and a state is that the state has no right to privacy.

After WikiLeaks – and later Edward Snowden – revealed top secret documents, theUS government went after these whistleblowers as well as the journalists who published the leaked information. Going after journalists for publishing information is considered undemocratic and yet it has become common practice in many democratic countries, even in Germany, as we learned in the summer of 2015.

The journalists at netzpolitik.org (a popular blog that covers Internet policy making) were accused of "*Landesverra*t" or treason against the nation-state. They had published a leaked document about plans by the "*Bundesamt für Verfassungschut*" or the Federal Office for the Protection of the Constitution, a German domestic security agency, to increase its Internet surveillance capacities. The state's attorney Harald Range investigated not only the source of the leak, but also any bloggers who reposted the information, even though their actions are supposedly protected under freedom of the press laws.

This led to a huge outcry by civil society and Germany's media managed to put a stop to the state's investigation. But this phenomenon has not disappeared and remains a major threat to our democracies. Indeed, states tend toward totalitarian behaviour whenever it involves their own secrets. So *Kontrollverlust* will only increase with the development of new digital technologies. which means the emergence of a new critical issue: The state must choose how it is going to deal with *Kontrollverlust*. It can either accept that it is going to have to relinquish control of its own secrets and become more transparent, or it will have to pursue a more totalitarian strategy in order to protect state secrets.

Many may find the notion of *Kontrollverlus*t annoying, especially since we have become aware of the nation-state's surveillance capacities. The state certainly benefits from these new developments in surveillance. But the very fact that we have become aware of its capacities means that the nation-state is in a much more precarious situation with regards to *Kontrollverlust*. Despite spending tens of billions of dollars on surveillance programs, the NSA was still unable to prevent the most important security breach in its history. Edward Snowden is proof positive that a nation may dramatically increase its surveillance capacities, but these efforts will not necessarily prevent the leaking of documents. Applying Lebanese-American scholar, Nassim Nicholas Taleb's concept of "fragile strategy", we note that secrecy has emerged as a very fragile strategy: Whenever a breach occurs, we are reminded of the many levels of the nation-state that are built on the foundation of secrecy and control of information flows. That is the very basis of its vulnerability.

Platforms: Second-Level Kontrollverlust

The first level of *Kontrollverlust* of the state is a loss of control over data, which hampers its ability to function. But this is not the only reason that the state is losing control: A second cause is the rise of platforms.

Some say that the state's loss of control has been absorbed by platform providers. Platforms are more than just corporations because they are the ones that provide the infrastructure for everything we do online and, in this way, they manage to accumulate a great deal of social, cultural and political power. And since most of us have decided to relinquish control over our data to them, they have emerged as the legitimate heirs of the nation-state.

But this doesn't only concern the nation-state because this transfer of power affects every institution (e.g., businesses, government authorities and bureaucracies) that functions as a representative of the people. It affects a broad variety of institutions that attempt to

manage the world by managing information flows.

First-level *Kontrollverlust* leads to various countermeasures being implemented in society. One effective strategy involves regaining control through the use of platforms, which can be described as controlled environments in an otherwise chaotic Internet situation. Platforms are centrally controlled and, instead of suppressing communication, they actually provide communication tools – but it requires following their set of rules and regulations. You can do anything you want on these platforms – as long as they give you the apps and tools to do so.

A good example of this is the music industry because it became the first victim – but also the first survivor – of *Kontrollverlust*. The music industry was not saved by the state, even though they fought illegal downloading by threatening users with new and increasingly stricter laws and regulations. However, the industry was saved by Apple, which created a music platform that was agnostic when it came to labels and publishers, provided a decent pricing scheme and unbundled songs from albums. It served as the first commercial attempt on the Internet to attract a broad range of music consumers and represents the dawn of a new age for the music industry.

But the industry was never satisfied with this lifeboat because it not only shattered their expectations, it also altered their beloved distribution system paradigm and meant a transfer of much of its former might to Apple, a technology company. The industry experienced it less as a victory and more as an occupation.

Another example is Facebook and the effect it had on our notions of privacy. Facebook is to privacy what iTunes is to the music business. It is actually the not-much-loved saviour of privacy in the age of *Kontrollverlust*. But just as iTunes recast the music distribution system, Facebook shattered traditional expectations regarding privacy. Facebook does not abide by a right to privacy. But Facebook offers sophisticated tools that allow individuals to control who can see what you've ever posted and who can see what.

Not unlike the music industry, we feel we've had our rights and our expected levels of control over our privacy plundered, for which we like to blame Facebook, when, in actuality, the very opposite is true. As long as you post and engage within Facebook's boundaries, one can achieve a certain level of privacy, which is a lot more than one finds on the rest of wild World Wide Web.

The important dichotomy involves, on the one hand, the Internet – a decentralised, open and anarchic network of data copiers – where there is no reasonable expectation of control over one's distribution channels of creative work, or one's privacy. On the other hand, we have the domesticated, closed and centrally controlled platforms, which basically represent the only places online with a modicum of control.

The move toward platform providers was initiated by *Kontrollverlust*, but was actually launched by another force – the network effect. There is a saying: come for the tools, stay for the network. People are initially attracted by the tools and then they want to do things such as listen to music or communicate with friends with those tools. When enough people are attracted to the tools, the second stage is launched: people become the main attraction. Today, everyone's on Facebook because everyone's on Facebook. The users are their own attraction. The music industry tried iTunes because they needed new tools with which to reach music consumers online. But as soon as the customers arrived, the tools became secondary. Later, you had to be on iTunes because this was where consumers could be found. That's only partly true today, however, since there are so many more services available such as Spotify, for example.

The network effect can be summed up thusly: Every participant in a network increases the value of that particular network. It behaves a lot like gravity: the more mass an object accumulates, the more gravity it attracts, which, in turn, leads to an accumulation of more

mass, which increases gravity and so on. Network effects equals positive feedback and serve as another source of power for the platforms. Like the Earth's gravity, platforms lock their users in. They become a necessary commodity for everyone else.

Another characteristic of platforms, in contrast to other institutions, is their global presence. Most of these platforms are almost as international as the Internet itself. Their growth is not limited by national borders; their market is the world. They gain a new kind of legitimacy as an international commodity for their users because the value of connecting everybody worldwide is not something the nation-state is equipped to compete with.

The Platform as a Tool of the State

The state is fully aware of these powers and tries to use them for its own agenda. In 2010, when Secretary of State Hillary Clinton gave her speech on Internet freedom, she described the vital role of the Internet and of Silicon Valley in the global democratisation process. She promised that the US would collaborate with the technology companies to provide the tools and manpower necessary to foster Internet freedom on a global level.

Nobody embodies this strategic collaboration better than Jared Cohen. As a State Department adviser under both Condoleezza Rice and Hillary Clinton, he was deeply involved in the details of this collaboration and as an Internet activist he created his own projects such as the NGO Movements.org, which trained members of the Egyptian opposition in the use of TOR and other cryptographic tools in the advent of the Arab Spring. Together with former Google CEO of, Eric Schmidt, he published *The New Digital Age: Re-shaping the Future of People, Nations and Business*, a book about future technologies and how they will affect society.

The Silicon Valley and State Department collaboration was at its peak in 2011, when the Arab Spring emerged. Facebook, Twitter and Google all supported the various revolutions and even collaborated with each other. Speak2Tweet is one examples: When Egyptian President Mubarak pulled the kill switch and disconnected his country from the Internet, Google engineers collaborated with their Twitter colleagues to establish a service that would translate audio messages into tweets. Speak2Tweet provided a telephone number where one could leave a voice message, which was then instantly tweeted to the Twitter account: @speak2tweet.

The emergence of the WikiLeaks scandal led to the disintegration of the Silicon Valley–Washington DC. relationship. Meanwhile, Edward Snowden's revelations in 2013 ensured that their relationship was irreparable. For instance, one of Snowden's revelations concerned PRISM, which is a clandestine NSA program (backed by a court of law) that monitored all of the communications handled by the largest Internet companies, including Microsoft, Yahoo!, Apple and Google. The revelations meant that Silicon Valley had to do damage control to preserve their images and prevent them from being perceieved as condoning the surveillance of their end-users. The once-praised relationship between Silicon Valley and Washington had become a total public relations disaster. The PRISM revelations showed that the government would not hesitate to fully utilise the growing power of the various Internet platforms for its own ends.

With 1.5 billion users, Facebook is currently the single largest organised social entity in the world. No nation-state can compete. Not long ago, they reached a goal of one billion people being logged in on a single day – on one website chatting, posting and communicating. Facebook is also the forum for massive public debates, which, of course, forms the very basis of the democratic process.

In the summer of 2015, Germany's Justice Minister, Heiko Maas, wrote a letter to Facebook to address the issue of the increase in right-wing riots occurring in eastern

Germany in reaction to the expected numbers of refugees that Germany was going to host. The political debate grew ugly and undignified, especially on social media, and *especially* on Facebook. Many activists tried to report Nazi and other racist hate speech, claiming it was a violation of Facebook's terms of service. But, in most of these cases, Facebook refused to act. This was when the Minister decided to intervene with his open letter, requesting that Facebook remove the racist content.This was indeed an interesting strategy by a state minister. Since Germany has no laws prohibiting hate speech, the justice minister felt it was his duty to fill the gap by demanding that Facebook intervene. Some people criticised Maas because they felt that he had been elected to resolve these issues politically – by introducing legislation that would limit hate speech, for instance – and not by passing the responsibility onto Facebook. But, on the other hand, demanding that Facebook take action made a lot of sense. Facebook's capacity to regulate speech is much greater, less bureaucratic and much swifter than any state legal process.

This seemingly desperate gesture is part of this odd European legal predicament called "the right to be forgotten". In 2014, the European Court ruled that – under certain conditions – Google would be compelled to redact its search index so that certain results would no longer show up when someone does a search of a specific person's name.

The conditions, however, are so ambiguous, that nobody really knows when this stipulation is applicable, which means that Google would have to decide on a case-by-case level. But there are literally tens of thousands of cases that emerge every month. Facebook established an advisory council of prominent figures such as Wikipedia founder, Jimmy Wales, and Germany's former Justice Minister, Sabine Läutheusser-Schnarrenberg to provide more legitimacy for this function. But, at the end of the day, it was up to Google to enforce the regulation. But since it has no clear mandate, Google ends up representing the interests of the state.

The conditions, however, are so ambiguous, that nobody really knows when this stipulation is applicable, which means that Google would have to decide on a case-by-case level. But there are literally tens of thousands of cases that emerge every month. Facebook established an advisory council of prominent figures such as Wikipedia founder, Jimmy Wales, and Germany's former Justice Minister, Sabine Läutheusser-Schnarrenberg to provide more legitimacy for this function. But, at the end of the day, it was up to Google to enforce the regulation. But since it has no clear mandate, Google ends up representing the interests of the state.

As we have noted earlier, the state always seeks to employ platforms to increase its own grip on power. These events are all part of the immense transition that society is undergoing and clearly acknowledge the power of platforms and conversely the declining power of nation-states.

The State vs. Platforms

One interesting development on the "Right to be forgotten" involves Läutheusser-Schnarrenberg's demand that accessibility to censored results be restricted to include areas beyond Europe's borders on a global level. In September 2015, France's National Commission on Computing and Liberty (CNIL) rejected Google's appeal that "right to be forgotten" legislation be limited only to Google's European domain name websites. We do not yet know how Google will respond to this ruling. And this is precisely where we encounter a basic structural problem when platforms are involved in the enactment of national legislation. While legislation applies to nation-states, a platform's actions may affect people on a global scale. Thus, this kind of conflict cannot be resolved as long as there is no global legislation.

For instance, Viennese lawyer and data privacy activist Max Schrems' "Europe vs. Facebook" campaign directly targets Facebook's legal status. The campaign attempted to

establish whether European laws on data protection could hold Facebook responsible, after it became clear that it was cooperating with US intelligence agencies in the gathering of the personal data of European citizens. But, of course, Facebook must abide by American laws and so it was in a position that meant either breaking American laws to comply with European laws, or break European laws to comply with American laws.

Since Snowden's revelations, there has been increased opposition towards Washington in Silicon Valley. Many platform providers, for instance, announced the implementation of end-to-end-encryption measures, which basically means encryption occurs prior to messages being sent to end-users, which means that even platform providers themselves cannot read the content.

Some American politicians' viewpoints, especially those arguing for increased national security, were simply outrageous. They were demanding backdoors or key escrow processes to the encryption software, which would allow American intelligence to gain access to any message if deemed necessary. They furthermore accused these companies of wanting to protect terrorists. In the summer of 2015, the Department of Justice obtained a court order demanding that Apple turn over text messages in real time. Apple replied that it couldn't comply since the conversations had been encrypted.

Just think about that for a minute: Silicon Valley corporations were encrypting their services in order to protect their users from their own government. The relationship between Washington and Silicon Valley had suddenly reached a low point.

But there are also more reasonable political voices. Michael Chertoff, former chief of Home Land Security, for instance, came out against the undermining of encryption software. He argued that as soon as the US government begins demanding a backdoor or second key for every encryption, then every government can demand the right to do the same, including China, Iran and various other dictatorships. The conclusion is obvious: One cannot simply apply national security demands to a global platform without eventually interfering with the laws of the land of every other nation-state.

The number of emerging conflicts between governments and platform providers continues to grow. From European data protection laws or antitrust laws to the prosecution of those who break national laws and issues regarding cooperation between the various players, many of these conflicts end up in a court of law. But some of these conflicts go even further.

China's War on Platforms

The irony seems to be that whenever a nation-state attempts to hamper a particular platform with national legislation it ends up further weakening its own legitimacy. Whatever it does, whatever it attempts, the nation-state tends to undermine its own puissance to the benefit of the platforms – with one exception: China.

In 2010, Google left China because of conflicts arising from its refusal to comply with China's censorship regulations. Facebook was also banned behind the Great Firewall and only LinkedIn continues to do business here. China has developed its own digital realm with it's own services. In a way, the Chinese government seems to have found a way to maintain its control over the data transmissions of it's citizens. But China pays a price for this level of control, which involve intense efforts at total surveillance and the enforcement of strict regulations of the industry and broad censorship laws.

But even this level of authority can never be total: Many Chinese people regularly use VPN (Virtual Private Network), which produces encrypted links to an Internet server, preferably to a server outside of China that serves as a proxy for that connection. The Chinese

government is unable to monitor these VPN connections and thus users can operate freely, in effect flouting China's censorship laws.

Some of China's practices seem counter-intuitive to us: Whenever Chinese students want to discuss politics freely, they switch from WeChat (which is very popular in China) to Facebook. In other words, they don't care that the NSA may intercept their messages, when the source of actual intimidation is your own government. In fact, there are some platforms that are simply too important even for China that it does not make sense for it to attempt to obstruct them with its Great Firewall. One of these platforms is Github.

Github is the number one resource for software developers worldwide. It is a social versioning system and code hosting platform, where most of the world's developers host their code, discuss programming issues, share their knowledge and code, and last but not least, companies hire developers based on their Github profiles. Banning Github from China would basically disconnect it from the rest of the programming world, including the latest software development and information technology.

This means that the Chinese government ends up tolerating numerous open source projects that are hosted on Github, despite the fact that some of these are directed against its national interests. Take the project "Great Fire", for instance, the only purpose of this project is to circumvent and undermine Chinese censorship. Any Chinese citizen can access it, with or without VPN, simply because China cannot afford to exclude Github from its Internet access.

But it seems that China has discovered a new strategy for battling this threat. The digital rights organisation, Citizen Lab, recently analysed a massive DDOS assault on Github's servers, which was mainly directed at the Great Fire project. A DOS (Denial of Service) attack is an attempt to flood a server with a deluge of useless requests, that is designed to bring a network down. while a distributed DOS (DDOS) simply means, that the flood of requests of a targeted system are generated by multiple attackers who behave in a coordinated, but decentralised manner. You can defend yourself against a DOS attack by simply blocking the IP address, where the attack is coming from. This strategy, however, doesn't work against a DDOS attack.

The Chinese government continues to monitor all Internet traffic exiting China because everything must pass through the Great Firewall, which manages to block a great deal of the daily requests and redirecting them to other locations.

In order to attack Github, the government simply gathered these massive amounts of blocked requests and redirected them to Github's servers. So, every internet user in China who attempted to reach a blocked service – Facebook for instance – at a particular moment, was unwittingly aiding China's cyber weaponry and so millions upon millions of requests per second were being sent to Github's servers. Citizen Lab referred to this effort as "the great cannon".

This scenario shows that some nation-states are literally at war with various platforms. Meanwhile, many platforms have created elaborate security measures to protect their end-users from their own governments. People – as citizens and as end-users – end up having to decide more and more frequently, who they can trust and this is not always an easy decision to make.

The transition has only just begun. There are many more developments on the horizon that will be implemented in an attempt to control platforms, to cooperate with these platforms or to totally impede these platforms. But in the end, everyone will have to deal with these platforms, because they are currently the only players who can provide a modicum of order and protection. But we the people (civil society) should remain very vigilant.

Over the centuries, we have managed to implement a variety of checks and balances, assign watchdogs and monitoring institutions to maintain a healthy balance between the power of the people and that of the nation-state. We have demanded that nation-states becomes more transparent and we demand to be heard. This is what we call democracy and perhaps this is the greatest technology of all.

Facebook is not a democracy; it's more like a feudal state with Mark Zuckerberg as it's reigning monarch. Even if you think he is a benevolent ruler with good intentions, one of the good guys, you cannot overlook the immense amount of power he exerts over our social lives and the potential political power he could wield. One of the most important challenges for the future will be the transformation of platforms into democratic institutions. The first step toward this goal would entail the implementation of a system of checks and balances. Google has taken an initial step in this direction with its creation of an advisory council. We should also wait to see what the results of the negotiations between Facebook and the German Justice Ministry on hate speech will produce. But all of this is only the beginning of what I call "domestic Internet politics", a politics for, from and of the Internet.

Michael Seemann studied cultural science in Lüneburg, Germany. In 2010 he started ctrl-verlust.net – a blog about theorie of losing control over data in the internet. It started as a blog project of the the German Newspaper *Frankfurter Allgemeine Zeitung* (FAZ) and was later run individually. In 2014 the latter topic was turned into a book: *Das Neue Spiel – Strategien für die Welt nach dem digitalen Kontrollverlust*. It was also partly translated into an English version with the title: *Digital Tailspin – 10 Rules for the Internet after Snowden*. Michael Seemann lives and writes in Berlin. He occasionally writes articles for several German magazines, newspapers and online news sites and also works as a lecturer, keynote speaker and consultant.

Crosslinks

Digital Tailspin : www.onlineopen.org/digital-tailspin
Culture of Control: www.onlineopen.org/culture-of-control

Tags

Control, Democracy, Media Society