Disconnect!

Everything &
Everybody
compulsorily
voluntarily
connected

and that's just
the beginning

Magazine for the promotion of resistance against the digital attack

VOLUME II: DISCONNECT – KEEP THE FUTURE UNWRITTEN

capulcu productions | Second Edition 2015

V.i.S.d.P. E. Schmidt | Am Zuckerberg 14 | 21984 Silikontal

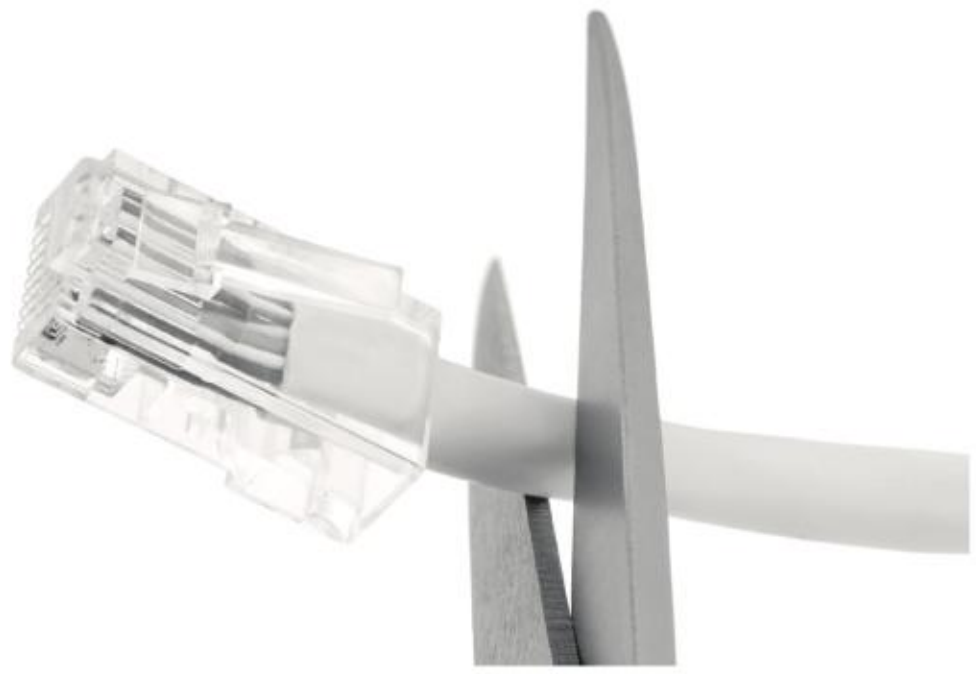
Capulcus means „robber“ or „hobo“. In 2013, turkish prime minister Erdogan tried to defame government opponents taking part in the broad revolts by calling them Capulcus. Instead of reporting on the Gezi-park protests in Istanbul that kicked off the insurrection, Erdogan showed a Penguin-documentary on national television. For this reason, the resistance made the penguin with a gasmask its symbol. From here on out, those that revolt are named Capulcus.

A digital version of this zine as well as responses and further texts relating to the technological attack can be found on our website **https://capulcu.blackblogs.org**. Feedback is always welcome. You can find the gpg-key to our email address **capulcu@nadir.org** can also be found on our website. To verify the authenticity of our key, we print the *fingerprint* here: AF52 0854 7EF1 711A F250 57CB D0D0 A3C5 DF30 9590 . Translation from the german done by a translation collective : **translationcollective.wordpress.com**

CONTENT

Disconnect - keep the future unwritten

Insufficient self-defense - break out of the future now!



For many years now, we've been assailed by a wave of technological attacks. We misconstrue this attack as a supposedly neutral „technological development" and play along willingly. It's time for a well-founded analysis, it's time for a plot against the dramatically increasing heteronomy. This brochure is our first collection of discussions and ideas relating to this theme. Our goal is to reject the grip of this ‚smart' attack and regain our sociality, creativity, autonomy - our life. We're looking for ways of self-assertiveness.

BREAK OUT OF THE FUTURE NOW!

With the first volume of this series „*Magazine for the promotion of resistance against the digital attack*", we published an introduction to digital self-defense. The recommendations contained therein are anything but convenient. By themselves, many held these suggestions to be unsuitable for daily use - we, on the contrary, find them to be absolutely necessary.

Concerning convenience, we don't want to emulate the maxims ‚comfort' and ‚velocity' any further, which have become ends in themselves. They are part of the undertow of a sea of data-hungry companies like Amazon, Facebook, Apple, Google, Twitter: power-conscious technocrats that strive for the complete and voluntary exposure of our data. Their ambition to completely record and analyze life's every movement so that it may be predicted and governed corresponds with the interests of their governmental ‚partner' organizations.

INSUFFICIENT SELF-DEFENSE

The technological methods of volume I *"Tails – The amnesic incognito live system"* helped us keep our heads above water while completing elementary political tasks: in communicating, researching, writing and publishing sensible documents. After

being forced to go undercover without revealing his whereabouts, even Edward Snowden used exactly these tools and live system to communicate. We are happy to see that some journalists are also using the system to protect their informants.

> ***Our refusal to participate in the endless digital transmissions and our self-defense against the digital access are nevertheless an insufficient attempt to divest ourselves from all-embracing control and heteronomy on a long term basis. A counter attack against the practice and ideology of this total acquisition seems to us to be both urgent and necessary.***

Unfortunately, if this counter attack is to have a chance, it requires some anticipation of future developments from our side. Because we have to break out of the future *now!* Now is the time to thwart their control-logic of Big Data animated self-optimization. Now is the time to break out of their form of functionalizing "connectedness". Now is the time to reveal and attack their smart arsenal, the mechanisms they use to record us, the mechanisms of our *future* control.

The Technological Attack

TECHNOLOGY WAS NEVER NEUTRAL AND STILL ISN'T

We must certainly make a fundamental distinction between a mere „invention" that can be useful, and an „innovation". The latter were inventions that became the basis of a widespread attack on the general public's forms of life and work. This process is still under way. Typically,innovations are the onset of a big cycle of reorganization and a renewal of the capitalist command. During the so-called ‚industrial revolution', the new machines (steam engine, automatic looms, e.g.) were

not only used to destroy outmoded forms of work and the ways of living based on those forms of work, but also to „stir up“ the entire population. They were parts of a widespread attack.

Defiant workers and crafts people that destroyed these machines were sentenced with capital punishment. The alliance between government and businessmen emancipated itself from skilled and craft work and instituted a new ruling tier against the aristocracy. During that time in England, they periodically employed militias of twelve thousand men for the sake of intimidation and counterinsurgency. Neither crafts people nor workers were opposed to an improvement of their work. What they opposed was becoming slaves of a development that would make them into appendages of the machines, and thereby becoming societally and politically debased. They fought against their repression and for a relative independence. They didn‘t want to be transformed into “human machines“. The fights were hard and bitter. The crafts people destroyed the machines reluctantly and only when they had to. The resistance wasn‘t blind– it was highly skilled. Destruction and riots were often only an eloquent means of bargaining politics and wages.

However, the „market“ was not the reason for this technological development, as is often claimed. On the contrary, the „market“ and its so-called political economy was first created as a part of this wave of violence. Marx called machines capital‘s “tools of war“. Till an old age, he maintained a conscious ambivalence towards a political-economical evaluation of technology.

The next wave of innovative violence was unleashed by the core of the new *weapons* and *machine industries* (Krupp, Borsig, Carnegie, US-Steel). The factory system was aimed against the movement of the 1840s, the so-called “pre-March” era. The subsequent wave of violence was started around the *electronic* and *chemical industries*. It was closely linked to the forms of behavioral disciplining and mental adjustment that Taylorism and Fordism achieved. Taylor, a pioneer of the new progressive-technocratic ruling tier, explicitly called this a „war“ against workers. His concept of force consisted in fragmenting the working, behavioral, and communications processes into well-defined individual operations, which were subsequently organized into programs. Said differently: algorithms. It was war and the expropriation of life at the same time.

From very early on Herbert Simon, a logician of organization, saw this as a starting point for the new information technologies. The historian Paul Josephson speaks of „technologies of brutal force“ that extend into all sectors of society, down to the colossal forms of environmental destruction. They were aimed against workers‘ insistence on autonomy and self-worth; in particular, that of the migrant workers. As recent studies show, these policies were enforced at a national scale during WWI,

and to a global scale during WWII.

Today this context is even clearer. The wave of attack launched by information technology had its first impetus in WWII as an expression of military competition. In the mid 1930s, the German Konrad Zuse was a forerunner of this process. In 1944, he was finally able to develop his Z4 computer to a certain point without the Nazis being able to benefit from it. By the end of the 1930s, just shortly after Zuse‘s inventions, the Anglo-American advances set in. They were able to push ahead of their German counterparts in a very short period of time, especially in the areas of information logic and software. While this whole scientific field was still bound up with military competition, the ingenious mathematician John von Neumann was pushing the development of the nuclear bomb forward. In his opinion, one thousand radiation deaths in nuclear tests were an acceptable price to pay for an American hegemony against Nazis and communists. The early giants of computing like „Colossus“, EDVAC, ENIAC were all children of war economies.

That these industries developed further shows us again how new entrepreneurial masters managed to emerge from a process of emancipation. The „treacherous eight“ separated themselves from Shockley Semiconductors, the first semiconductor company. They didn‘t want to put up with the autocratic Shockley‘s uncompromising management anymore. Among them was Gordon Moore (who later founded Intel and is the author of „Moore’s law“, which states that the processing power doubles roughly every two years). Horizontal hierarchies, co-operation, and fun was their credo.It is very fitting that Moore‘s favorite film was „Mutiny on the Bounty“. It was the story of a personal and sexual emancipation from the hard autocracy of a relentless captain. The movie was a Zeitgeist project, and completely fucked up the historical facts.

Following this, the historical-technological unleashing was embedded in a broad cultural and in particular youth-centered emancipation movement. It‘s musical expression was rythm‘n‘ blues, Elvis, and the flourishing pop music. They began to tear up the net of social discipline created by Fordism and Taylorism. This process was intensified in the revolts of 1968, which aimed at all the different dimensions of the industrial society and more generally at society as whole. These revolts were the real reason for the general societal and economic crisis. Still to this day, its emancipatory traces have not been fully erased and continue to live on in individual strands such as the hacker movement.

After the new IT economy‘s greed for power and money killed the emancipatory spirit in the 1990s, the American central bank under Greenspan, and Clinton‘s economic advisers under Summers, attacked the US- American workers‘ bargaining power (what little of it was left after the Reagan era) and their forms of living. In

1995, Greenspan and Summers launched a specific process of „creative destruction“ - the destruction of the old world and the creation of a new one. At the same time, they aimed to make American power a leader in world technology. After succeeding in doing so, they procured a fifteen year head-start for the US. This attack is far from over.

> ***New research states that due to this technological change approximately 50% of the jobs will disappear in the next one to two decades in the US alone. All this, combined with an enormous increase in technologically induced capitalist power.***

The effects of this new wealth are mirrored in the personalized wealth of the top-level employees in IT sectors and technologically-upgraded banks. This goes hand in hand with a dramatic devaluation of the former middle class and the minimum wage service sector. The same can be said about the effect wealth has on the society as a whole: California‘s gross national product (Silicon Valley) has outrun that of Brazil and Russia. The forceful and powerful character of information technologies becomes more visible:

> ***Whoever writes the software determines the application of the processes, including their social ramifications.***

All in all we are witnessing yet another historic wave of violence and power, this time with the prospect of an enormous intensification. For them it is just the beginning. Basically, Taylor‘s „war of scientific management“ brings all of this to a new level.

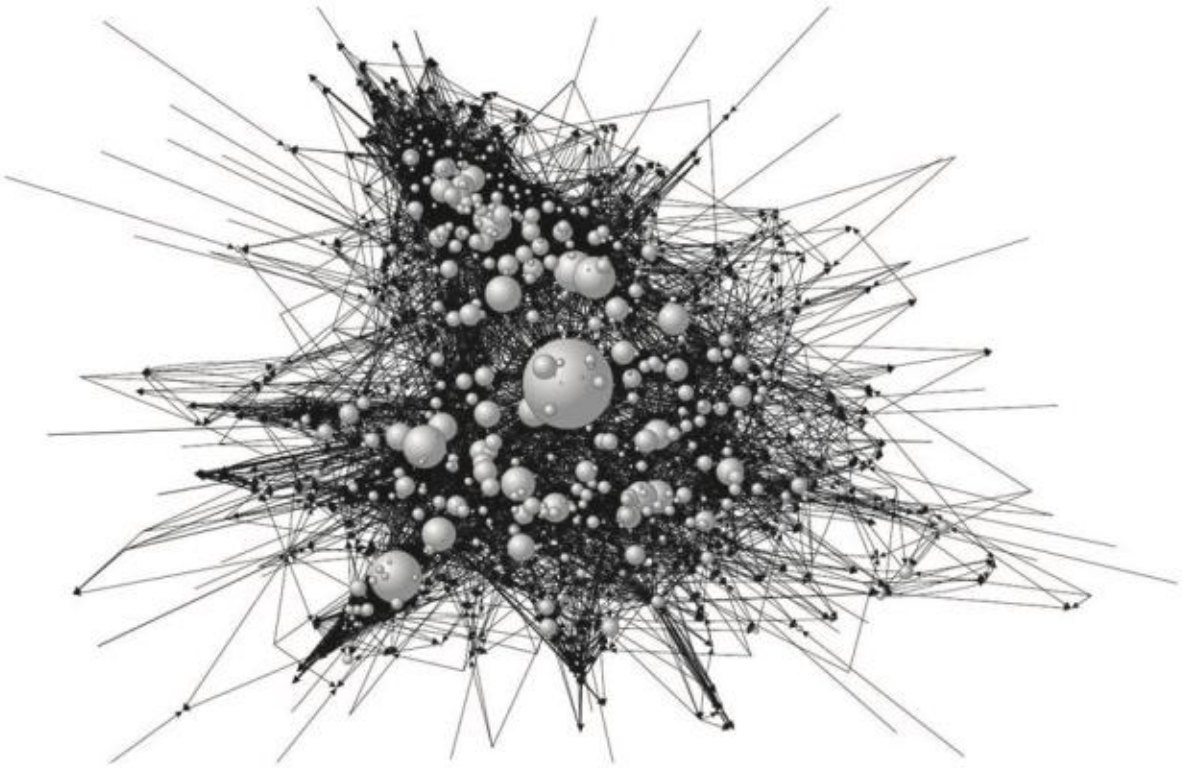
In this brochure, we trace the new wave of technological attacks along individual paths and facets. We do so in an exemplary manner, not systematically. For their history is not systematic; it proceeds by “trial and error”. This history will only appear to be logical in retrospect, after all the history books are cobbled together. Or maybe histories, depending on the point of view. But they are not over yet, they‘ve just begun.

In its early thrusts the social, technological, and economic conflicts always reproduced themselves on new levels. In the end phases, the social revolution seemed to have lost. But this is only an illusion. It is an optical illusion produced by a false perspective. The social revolution didn’t lose, it just hasn’t won yet.

We have purposely refused a ‚common thread‘ that would unify our hypothetical and speculative logic of development. Neither do we suggest any common threads for social revolution, nor for the technological grasp. We just offer tools. “We” are not homogenous and we follow these developments in noticeably different ways. We hope that a discussion with you will help construe new interpretations and analogies between

the different strands of the attack. The common thread wouldn't be the right story anyways. Above all the red thread would impose itself unnecessarily on our minds, souls and bodies that strive for liberation and revolutionary self-organization despite the abundance of technological tinsels that decorate the impoverished world of our adversaries.

The Destruction of Social Life



There's only have one rating that's even worse than a very awful rating – no rating at all! (M. Elsberg - ZERO)

In mid-August 2014 the weekly newspaper „*Die Zeit*" had an article that described Googles' views of the future in extensive detail. Lots of people started to worry because these views did not include the state and law. Strictly speaking, the article claimed that the state should be deregulated by a system run by Google. Everything that could block data streams or get in the way of the limitless developments of IT and cybernetic intelligence was deemed outdated. As the surprised reader could read, the prototype of the new world will be created on the oceans, separated from territories and states. The net will be the center of a world located on artificial islands inhabited by like-minded people. Nerds will work on perfecting these nets. Flexible algorithms - codes - will replace inflexible civil „liberties". People will be happy and satisfied, at least those who can make themselves comfortable in the nets' nests.

It is paradise. A surrounding that leaves nothing to be desired. Smoked tofu will not fly directly into your mouth, but it will be served by a robot before you even think of ordering it. Your health app recognized that tofu would hit the spot for you right now. Your smartphone already chose the movie for your necessary dis-

traction. Later on, the comfy-chair will slide back because it knows that you need a little nap now. You will work during the times allocated to you by your personal tablet. Your ratings get better and better, almost reaching the optimum. But wasn't the optimum lower the day before, you ask yourself. The robot serves you a drink, the thought vanishes. Tomorrow you will travel to Honduras, the mainland, for a week-long holiday.

Honduras? Do they have internet there, do apps even work there? Who will tell you your fitness program in the morning and about what you should do today? Will you eat the right food without the apps? Isn't your personal profile getting completely messed up? Can you recognize dangerous people on the streets without the face recognition of your smart glasses? Forget your holiday in Honduras, the fear of being offline overwhelms you.

A fear that is shared by many. Without internet they cannot work, communicate, shop, watch movies and listen to music anymore - „without" lots of people feel isolated and lonely. A world without internet is unthinkable. Google, a company with a stock-market price twice as high as that of Volkswagen, Mercedes Benz and BMW combined, is certainly working to make that the case. The question what makes the IT sector that valuable is easy to answer. It is billions of data that are „donated" voluntarily by millions of people every day. Selling this data and transforming it into algorithms is worth billions. That is because they are giving information about the life of individuals, their desires and needs. This information can be transformed into goods. They also allow desires to be depicted before their emergence and thereby marketed to specific individuals.

BIG BROTHER IS NO LONGER A THREAT, BUT A RELIABLE FRIEND

Millions of users don't worry about that. They not only have „nothing" to hide but also trust the net in all spheres of life. Which job should I apply for? Is it good for me, to meet X now? Which bargain should I take advantage of? Even the most intimate questions about health are answered by the net. Gradually I decide less and less. The apps that should be helping me have slowly taken over command– and I feel better and better?

Advertising successfully influenced our lives for decades by making suggestions. What is new and decisive is that the „suggestions" we're experiencing now are fit for my personal life. They do not address millions of people with a single ad as conventional advertising does. It makes a difference if people are influenced „from the outside" or if apps record their actions, thinking and feeling to influence them individually. That's because these suggestions follow a statistical method, a technological processing that wants to influence and manipulate them on a massive scale. They make you believe it's an individualized piece of advice, but in fact it's

the exact opposite. The recommendations are statistical averages made up of like-minded people. Surveillance, control and acquisition lead to a manipulative rating and reward system that covers all areas of life. This form of self-optimization disconnects the individual more and more from real social contacts. Apps determine life and are becoming an accompanying feature.

CREATIVE DESTRUCTION

The interesting question of why users trust machines more than people is difficult to answer. It is easier to describe the commercial profit of this attitude. Economist J. Schumpeter said that capitalism destroys old values to collect energies for its next attacks. „Creative destruction" is his term for forces that shake the basics of social relations to their core. Considering the consequences of war, this is easy to understand.

People are being killed, hurt and traumatized. They flee, are torn from their old relationships and live as refugees under lousy conditions searching for new ways of survival. Houses, villages, factories and infrastructure are bombed and have to be rebuilt. It is the time of machos and wartime profiteers who fill the power vacuums and profit massively from new conditions. The old familial and neighborhood relations no longer exist. The residents are scattered all over the place. To escape hunger, they labor in factories producing for the world market, in refugee camps and slums. They are confronted with a new form of capitalist exploitation under harsh conditions. Women and children are even more exposed to violent attacks from men. They are all forced fend for themselves alone. In this foreign environment, insecurity and distrust rule every day life. The rest of their social, mutual responsibilities waste away under these living conditions. Attitudes and mindsets change rapidly.

In Rojava (a Kurdish area in northwestern Syria) people are trying to break out of this capitalist logic of violence. Lots of people went there to escape the war zone. They built self-organized communities that resist government and religious enemies and overcome patriarchal hierarchies. Kurdish fighters were able to disperse the occupying troops of ISIL out of the city of Kobane, although suffering heavy losses. A city in ruins was left behind. A result that was not inconvenient for the „defense coalition" consisting of the USA, the EU, Saudi Arabia and Turkey, who joined last-minute.

GREED - PROFIT - FEAR

Capitalist „crises"- such as the so-called financial crisis - cause drastic social changes beneath the threshold of war. After eight years of crisis, lots of family networks

have broken down in the metropolis because of the stress caused by unemployment. This can be seen clearly in Spain, Portugal and Greece. The old have to fight for their daily existence, while the young seek their fortunes abroad. In rich countries the process of gentrification leads to evictions of poor people. „Deindustrialisation" made them redundant and forced them to live in the wasteland of suburban ghettos far away from their cities' home districts.

This destruction is „creative" in multiple aspects: their lives get lonelier and lonelier, social relationships are stunted, they have to work for starvation wages and their cost of living rises.

It is a remarkable phenomenon that greed, or rather being to cheap to spend money, is far less common in poor people than in rich ones. Obviously, someone who worked their way out of poverty hardly ever looks back but has the unconditional will to climb up the ladder. This way a private conversation, a job application, even an internet date becomes a competition against others. I check everything to see if I am being cheated and to see if I can cheat somebody unnoticed. There are no restrictions against cheating others to climb up the ladder

It is probably this knowledge that the IT industry uses. „These apps do not need egoists, they produce them", knows even Frank Schirrmacher, editor of Frankfurter Allgemeine Zeitung, a leading German daily newspaper.

DEMOCRACY CONFORMING WITH THE MARKET

Chancellor Merkel put her vision of the future in a nutshell: Democracy has to conform with the market and is subordinated to it. In saying so, she follows Google's aforementioned visions and the neoliberals' creed.

They have their eyes set firmly on a common purpose: the market. The economy should be set free from the chains of state and law. The way should be cleared for capitalism to turn human beings into resources that are exploitable day and night. The „eight-hour" day in the cities became a ridiculous relic of a long gone past. „Smart" life establishes an indissoluble connection to data-zombies. There is no life outside of these networks, market participants say.

This brave new world does not need humane social relationships. They are going to be replaced step by step by „social media" and countless apps offered. Users are producers and consumers at the same time. It is a world that fulfills the patriarchal wish for a society ruled by technology. The illusion that humans control the machines bursts by using a smartphone. While some users still believe that the internet grants their wishes, they do not recognize that „their" hits are created by apps or more accurately: their wishes already have been created.

BEING DISSIDENT

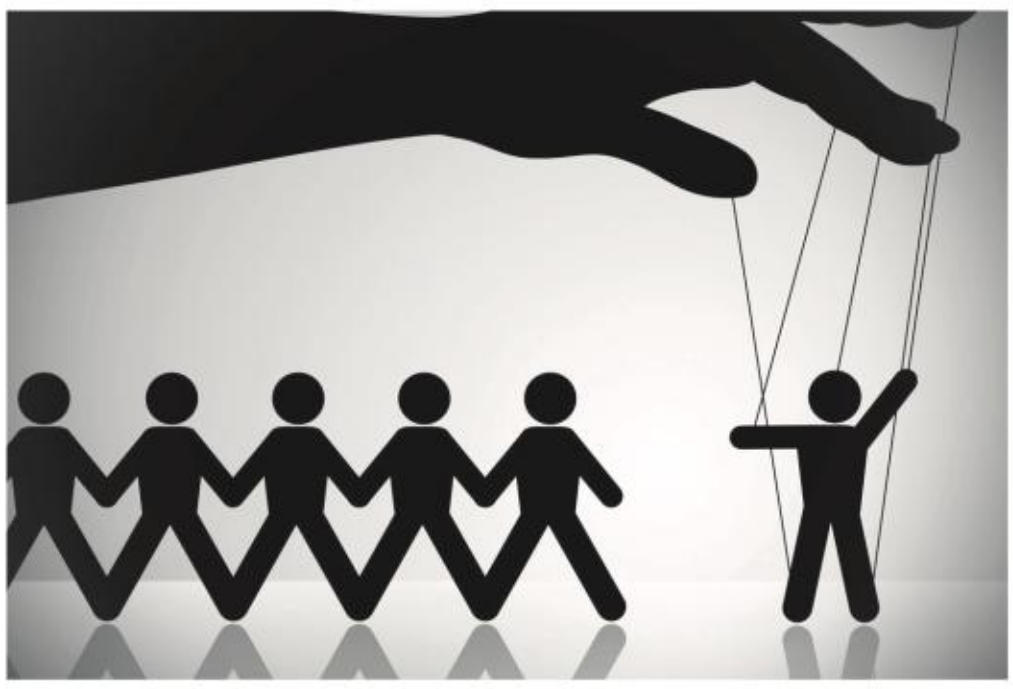
The net is the market of all possibilities. Whoever doesn't subordinate to it refuses progress and hasn't understood anything. Before we defend ourselves against this imputation, we should take some time to think about what is wrong with not becoming donors, producers and/or consumers of data for Google and associates. Do I want to follow the apps „advice" and take my part in the creative destruction that makes my life a social wasteland? Do I want to take part in the process that makes humans into machines that are streamlined to the market?

It makes sense to be dissident and when ever possible to use the internet anonymously and with encryption. Those who choose to live as dissidents may be able to answer the question of why users trust machines more than humans. Is this because these humans already have become machines?

> *„There are a lot of turtles out there trying to avoid becoming roadkill on the information highway ... The turtles represent the real threat to the stability of this whole movement toward high-tech, free-market, global capitalism" says IT-fan and journalist Th. Friedman.*

From Total Acquisition to Manipulation

WHO GETS WHAT INFORMATION IN THE ALWAYS-ON SOCIETY?



> *„The world is not sliding, but galloping into a new transnational dystopia. This development has not been properly recognized outside of national security circles. It has been hidden by secrecy, complexity and scale. The internet, our greatest tool of emancipation, has been transformed into the most dangerous facilitator of totalitarianism we have ever seen. The internet is a threat to human civilization. These transformations*

> ***have come about silently, because those who know what is going on work in the global surveillance industry and have no incentives to speak out. Left to its own trajectory, within a few years, global civilization will be a postmodern surveillance dystopia, from which escape for all but the most skilled individuals will be impossible. In fact, we may already be there.“*** (Cypherpunks, Freedom and the Future of the Internet, 2012 – before the Snowden revelations)

Our standpoints, which we share via our cell phones designate our ‚usual' locations. When we spend money with our credit, EC, or loyalty cards , we leave behind an individual fingerprint of our daily life in the amount, place, and intended use of our expenses. Telephone, Email, Twitter and Facebook provide a nearly complete sociogram of our contacts: a simple software uses a graphic to represent the question „who is associated with who and how intensively?“. Keywords and semantic analyses of unencrypted communication disclose the character of particular social relationships as well as our individual patterns of speech.

An analysis of only a few months can depict our individual ‚average behavior' to a level of sufficient precision, making every one of our ‚normal' behaviors predictable. Deviations from these behaviors are easy to detect and trigger the attention of the snoopy authorities and economic data exploiters. The sobering fact about all of this is that none of the aforementioned methods of analysis require the immediate effort of people. Nobody has to be explicitly interested in us. Through the data centers of the internet connection nodes and data farms, self-learning algorithms manage the analysis automatically and parallel for around 3 billion voluntary data suppliers worldwide at the moment. It is a gigantic control apparatus that isn't satisfied with the acquisition of data alone. The now imminent linking-up of all controllable objects around us, the precognition of what we desire, of what we want to do takes it to the next level.

The introduction of these omnipresent net technologies that weave everything and everyone together are so successful because their advantages are much more obvious and immediate than the problems they create. The latter will only become noticeable when the widespread use of these technologies is already established– by that time it's usually too late, since the normal reaction is familiarization instead of resistance. This is encouraged by a Zeitgeist that makes us believe that the idea of the private sphere is an obsolete category. The offensive influence of this Zeitgeist in public debates is a part of the technological attack.

We all have but a vague understanding of what's happening to us. We are already completely exposed to the everyday steering of those who gather and analyze our data, and use the information gathered to process our individualized news feeds. However for many, the perceived threat is contained within the range of mode-

rately useful to annoying advertisements which are individualized based on our Google searches, the websites we‘ve visited, and the online purchases we‘ve made in the last years. But it‘s nothing bad– better personalized than completely random advertisements, say many users.

That two different Google users receive different results for the exact same search is something worth thinking about. Wasn’t equal access to a ‚collectively‘ compiled knowledge of the world one of the foundational pillars of the self-proclaimed digital enlighteners?

In 2014, the erasure of Google’s search-result lists was enforced (in exceptional cases). Many celebrated this as a legal victory against the data kraken Google in favor of a popularly-demanded ‚oblivion on the internet‘. When we ask Google to erase (defamatory) data, we indicate our vulnerability and give the corporation and all its snooping authorities a considerable amount of power. When we request for our data to be erased, we draw a lot of attention to ourselves. Meanwhile, the extensive *Google-blacklists* can be more valuable than other indicators for measuring an individual’s credit rating.

With such precise attention to detail, personal profiles enable a subtle yet highly effective manipulation of users. Google‘s openly declared goal is to expand its supremacy as a smart manipulative life companion. Soon we won‘t use Google to search for terms, but rather ask it what to do next, says Google‘s chairman Eric Schmidt. In Schmidt’s self-conscious imagination, Google will soon organize our entire environment. This complex environment requires an organization of daily life optimized by algorithms, at least for all of those that want to move ‚forward‘.

Google has already dedicated an entire branch to the *Google Brain*, a project that will examine the decision-making process and create a replica of the human brain. In contrast to Orwell’s classical surveillance state, this project‘s central aim is not the repressive limitation of thought‘s free play, for example, the suppression of a vocabulary that would enable ‘thought-crime’. On the contrary, rather than silencing people, the ‚digital panopticon‘ a la Google, Facebook and co. encourages everybody to be ‚*always on*‘ - the digital permanent transmission. Instead of mandating silence, the new power encourages everyone to tend towards an exhibtionistic self-optimization in a smart fashion. Rather than being made ostensibly docile, people are made dependent. To this end, rather than a threatening, repressive grimace the colorful, friendly world of Apps is utilized. Comfortable creativity- and efficiency-increasing auxiliary programs on our smartphones work together with additional sensors connected via bluetooth to stimulate us into ‚liberal‘ self-exposure.

Yet that doesn‘t mean that the classic censorship will be entirely removed from the repertoire. The USA has recently described internet connection for everybody to be a component of people‘s basic needs (next to water and electricity). Yet nonetheless the targeted, partial or complete shutdown of the internet as a communication infrastructure is a permanent part of a counterinsurgency strategy in the *cyberwar* declared by a permanent state of exception. Which by the way is the same strategy of stabilization as was used in the 2001 declared (end never revoked) ‚state of exception‘ of the *war on terror* .

This also works preventatively and in a more subtle manner: on August 9th, 2014, 18- year old Michael Brown was shot dead by a police officer in Ferguson, Missouri. A patrol officer stopped him because he dared to walk on the street instead of the sidewalk. During the discussion a shot was fired from the police car. Brown ran away and was shot from behind by a police officer. Michael Brown was unarmed and black.

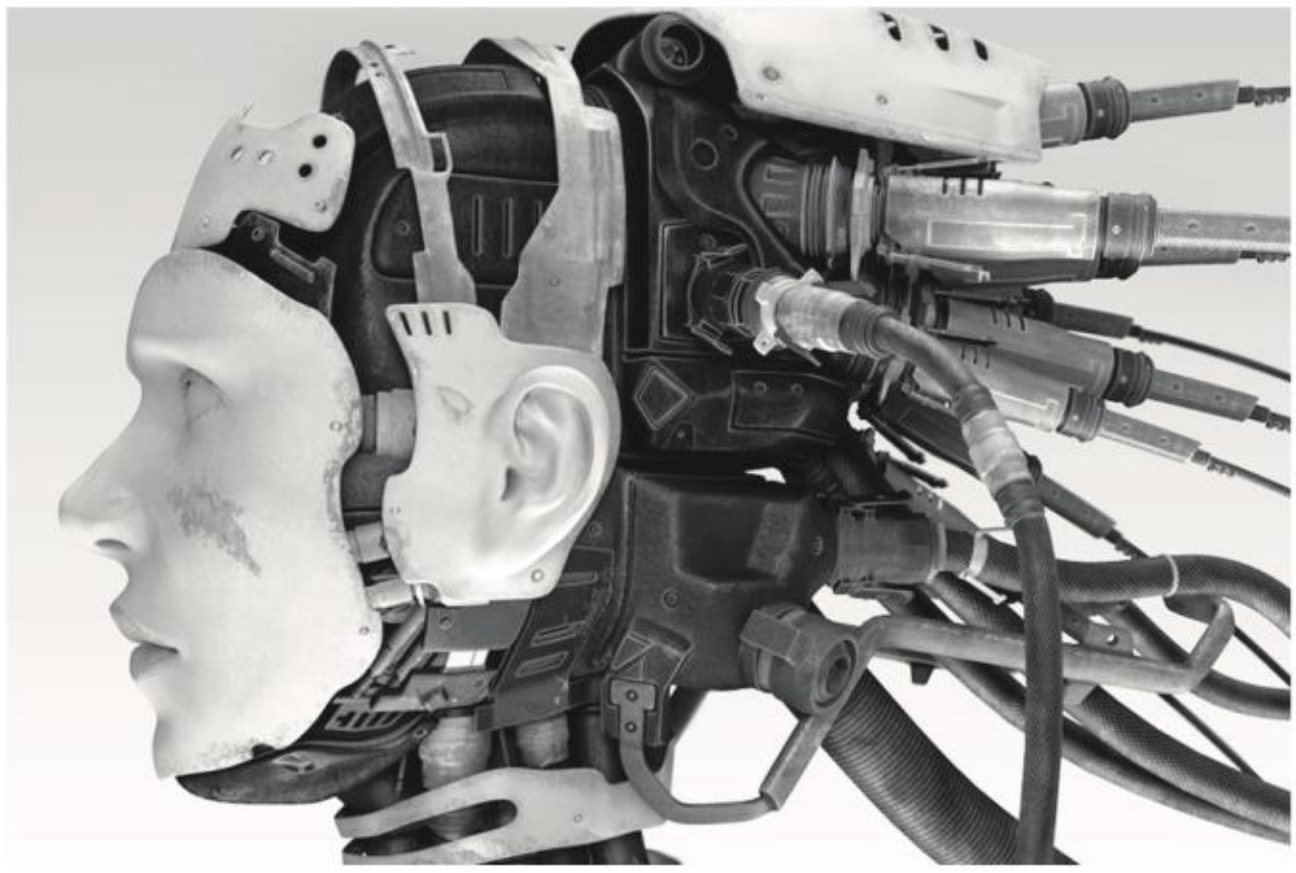
Already on the next day, people from the city‘s the black community gathered for a vigil that was met immediately with 150 police in riot gear. The mood heated up, the situation got out of control, there were street battles and looting. On August 11th and 12th, the police used tanks, flash grenades, smoke bombs, teargas and rubber bullets against the uproarious crowd. The images of the martial combat of the insurrection were spread worldwide through the media and of course by social media. But not through all social networks equally.

Zeynep Tufekci, professor at the university of North Carolina examines political power through the algorithmic filtering of messages. In a contribution to the blogging portal *Medium* she claimed that Ferguson hardly appeared in her Facebook-stream, while on Twitter there was almost no other topic. However, that wasn‘t because people on Facebook didn‘t write anything about it.

The *Edgerank*-algorithm, which spreads news according to personal relevance seems to have simply filtered the topic out...

Machines that control humans

An unhindered flow of information to maintain the stability of the system



You stand on the street and use your smartphone to take a picture of a vehicle that is parked unlawfully in a handicapped spot. In the same moment the position of your smart phone is recorded. The public space' s video surveillance also documents your act.

You are pursuer and pursued at the same time. Your photograph lands in the cloud and the prosecution agencies have access to it. You are totally inside a feedback loop, you have become the transmitters of information in the best sense of cybernetics. Congratulations. you've done unpaid work that had to be done by public affairs employees before. Now you are competing with these people for employment opportunities. Of course you hope that this denunciation will reflect positively on your rating. Or not?

The significance of information has changed drastically since the micro electronic revolution. Every time we disclose information, every time we give a sign of life we serve the market. Directly or indirectly, consciously or unconsciously we are part of a cybernetic capitalism. Why cybernetic?

Cybernetics is a field of research that makes comparative observations about regularities in processes of control and regulation (in technology, biology, and sociology). Cybernetic assumes that it's necessary to gather information in order to create stability. This information will be used to adjust the „system". For example: In order to stand upright, the flow of information connected to a person's nerves has to be quick enough. This information grants the corrections that enable us to use muscle contractions to balance ourselves.

Sociocybernetics uses rigorous methodical research to plan the future of the individually operating human being. Cybernetics takes account of all the information about humans that is able to be planned. The seemingly free planning and action of humans is thus disruptive. Roughly speaking, cybernetics is about stability of the streams and their flow into the biopolitical tissue.

The rapid recovery of states of equilibrium requires that deviations be traced back to their origin. These deviations are then corrected in a decentralized way. Sociocybernetics sees the individual as a site of feedback and self-disciplining personality. The goal is a new configuration of the individual or collective subject in sense of an emptying. Everyone has to become a bodiless shell, become the best possible conductor of social communications, a site of infinite feedback that follows a trouble-free routine.

So why is it happening? Based on the previous cyclical crises of capitalism, it appears that capitalism has again readjusted its capacity to disintegrate and seek profit. No growth without destruction. A society threatened with constant decay can be dominated much more easily if there are information networks, a virtual „autonomous nervous system". For the contemporary constitution of capitalism that means:

Information has become the commodity with the most promising future.

The techniques for adjusting supply and demand originated between the 1930s and 1970s. Now they have become more sophisticated, shortened and decentralized since they are materialized in computer processes. The internet makes it possible to recognize a consumer's individual preferences, to steer them through advertisement and to try out previously unnecessary product trends. The unlimited hunger for data combines an analysis of the relationship between a customer's whereabouts and their purchasing habits. How long or often do I linger in front of which store window, which products am I interested in online, how often have I been to which shop, what kind of advertisement will I get... in the end all the available data will be used in the rat-race to sell a product more quickly than competitors.

The communication technologies in trade and financial sectors have been automated. On October 5th, 2011 a bomb threat reached Frankfurter stock exchange and the building had to be evacuated. But this did not have any impact on the stock market's trade, since the transactions were being run by a computer program called *xetra*.

On another level, all the information about economic stakeholder's behaviors circulates in the form of titles. These titles are assessments of information that are in turn traded themselves. In the stock exchange, everyone who participates in the production of capitalist value carries a real time feedback loop.

On the real as well as virtual markets, every transaction leads to a circulation of information about the subjects and objects of the exchange. The importance of this information has exceeded the simple setting of a price.

> *Today, two thirds of the industrialized countries' labor force are working in the economic sectors of information, communications, and control.*

On the one hand information is a factor of production that is different from labor and capital. In the form of knowledge, technological innovation, or broadened competencies, it is decisive for „growth". On the other hand the sector specializing in the production of information is growing constantly. Both tendencies reinforce each other. Information is both a requirement and an outcome of work.

Information become a treasure that has to be extracted and accumulated.

> *Today the biggest share of the profits is made with the predictability of the future.*

Cybernetic capitalism has made its continuous 'balance' and growth dependent on its ability to control.

> *Therefore far more than shortage, insecurity has become the core of the current economy.*

Only by accelerating the production-consumption cycle, the production process and the production of goods secure profits (by just-in-time production and the elimination of storage). The impact of acceleration also becomes apparent in the stock exchange. Profits are made in a range of tenths of milliseconds. This means that it's important to have the shortest cables to the host computer.

> *The acceleration of the circulation of information as a commodity has an enormous importance for the balance of the system. It has become a factor of wealth.*

Production – consumption, the ever faster acquisition and control of trends. Total transparency is necessary to provide the system with stability. Preferably in real time.

After the crisis of 1929 a system of information about economic activities was created for regulation. Today's process of social self-regulation in the economy is based on that valorization (setting-into-value) of information. The fact that value can be extracted as information about information shows the relevance of cybernetics. In the course of the century, the relationship between capitalism and cybernetics has shifted. Has capitalism been transformed into an assistant of cybernetics?

The feigned equilibrium that is talked about from a cybernetic-capitalistic point of view is history itself, the political moment of human action. To the same extent that we accept higher rents, longer working hours, additional payments in the health sector, pension funds that are speculated on on the stock market, friendship as commodity, we take part in the balance and „growth" of cybernetic capitalism. We are already regulating ourselves.

> *When we heed to the machines' commands to communicate, we take part in the stability of contemporary capitalism.*

Its aspiration for total transparency (in real time) is the foundation of the ongoing setting-into-value of information. The permanent transmission of data about all manifestations of our life is just another step towards the enslavement of humans by machines. The further the sensors get into the bio-politic fabric, into the lives of humans, the further humans will be subject to the diktat of algorithmic machines.

Refuse the transmission. Switch off, throw away, destroy everything that seems convenient.

No connection. Getting rid of the seemingly technological aids opens a space for improvisation. The reappropriation of stolen abilities. Is it important to share a point of view, to „like" a protest, to inform the persecuting offices of my discontent? How would we act if the net broke down? Shouldn't we spend our time creating and expanding invisible spaces where encounters can happen? Spaces that are not monitored by sensors? For a collective rebellion against the acceleration, the transparency, the commoditfication life.

Slowness breaks interrupts their streams of data. It is necessary for our relationships with each other. It is an attack on the essence and process of cybernetics. Time is our ally. No recognition and no approval. The refusal to give feedback. When individuals forget about self-discipline and leave their assigned function behind, they destroy the fabric of control

People that crash machines

RESISTANCE AGAINST A SELF-REGULATED INFORMATION SOCIETY

We know that you won't like the following description, since you *consciously* remain in the cybernetic paradigm of thought, in the models they use to describe the world, in *their* logic of parametrization and seeing every disturbance as an opportunity to increase their ability to rule.

To us it's clear that revolutionary uproar will never be conceivable in *their* system-language. The contagious moment, the intrusion of heterogeneity, of the outside into a situation leads to a rupture with their logic, a rupture with our self-imposed coercion to conformism.

Nevertheless, the chances and effects of resistance can be examined from within their model. We engage with the cybernetic model because it is not only their preferred mode of representation; at the same time it's their instrument of reaction, control, and the state of exception. It describes their reaction to our resistance: they don't change this model of thinking or behaving even if large parts of the population take part in social upheavals. Their engineering-logic of *social physics* is molded by an algorithmic description of individual patterns of behavior. To the end of being able to steer these behaviors, they are put in contact with other individuals' behaviors.

The system they test out in normal conditions (by all means with a view to a revolt) uses so-called *critical parameters* to try to detect which possible disorders (in simulations and singular praxis-examples) could occur. The system's reaction to the variations of these critical parameters is then examined, with the end of stabilizing the system. Non-linear systems that give feedback allow the possibility (under certain ‚critical' conditions) for ‚chaotic' or unpredictable states. From their point of view, it's necessary to keep this probability as low as possible.

What would a break with the cybernetic system look like?

1) REFUSAL– WITHDRAWAL FROM THE PERMANENT (UNENCRYPTED) DIGITAL TRANSMISSION

Withdraw into the fog and retract yourself from their tentacles of control. Create zones of ‚non-communication' and refuse their offers to participate in or give feedback to their control circuits. Refuse the controlled transmission and augmentation of information. Don't take part in the horizontal hierarchies of their cybernetic organization models nor in the endless staged (citizen) negotiations at (network-) round tables that include more and more players.

Don't be a work node in their net and withdraw from their entirely surveilled communication. What does that mean concretely? We refer you to the methods of encryption, digital refusal, and use of multiple identities recommended in the text *„We haven't lost, we just haven't won yet"*.

2) HACK/ SABOTAGE THE INFORMATIONAL NERVE-SYSTEM.

Resistant noise is that which can't be reinterpreted as a productive disruption and incorporated as part of the learning process to optimize the system. It creates a loss of information. The noise reduces the information content and can lead to turbulence or idling in their control circuits. In order to make the turbulence controllable and to stabilize the system, their control circuits will be enlarged. Nodes can be broken away from, the circulation of data can be interrupted. During an idling, all the signals are drowned out in the disorder caused by the noise– no more meaningful feedback is possible in this situation. That means a recession in the network.

The structure of the internet as a material network is made in such a way that data packets traveling from A to B are able to bypass local disruptions on their direct route by inquiring into the availability of possible escape routes. However, if many channels drown the original information in noise, or completely malfunction, the information can find very few (if any at all) ways in the otherwise finely-woven net between sender and receiver. If the communication is disrupted locally at many places, these decentralized disruptions create bandwidth- bottlenecks or even the collapse of entire subnetworks.

3) OVERDRIVE– FRICTIONLESS STRENGTHENING OF FEEDBACK.

You know what happens when a microphone is held right up to a loudspeaker. The microphone's signal is strengthened and echoed by the speaker. This strengthened

signal is received again from the microphone and strengthened again etc. If no or only a little bit of absorption is used, then an over-amplified feedback occurs– it screeches very loudly, and the amplifier‘s system is jammed.

The race between mass communication and mass surveillance functions similarly. If critical messages and voices within mass communication disseminate at a high velocity, then it becomes impossible to control the information system either th-rough repression (censoring) or dissipation (counter-information). Such a loss of control certainly requires an exceptional situation, in which a ‚mass consensus‘ manufactured in a short time makes for such a quick understanding and dissemi-nation.

Let‘s take the example of the 2008 revolts in Egypt. At the time, a Facebook group helped the events of the insurrection spread lightning-fast in the framework of a call out for a general strike. The activists of the first hours could inform each other quickly and the feedback of the masses was just as quickly noticeable. The gover-nment was surprised– mass surveillance, state censorship and false information followed directly on the heels of the spread of the insurrectionary fervor. However, many arrests were made after an analysis of the social networks!

In the following Egyptian revolution of 2011 a pamphlet, a type of revolutionary handbook called „*How to Protest Intelligently*“ played a central role. *“Do not use Twitter or Facebook to distribute the manual*“ was written on the first and last pages of the pamphlet. Nonetheless the handbook was spread en masse via Facebook and Twitter. Luckily, this happened without fatal consequences, since the insurrection was ‚successful‘. Otherwise thousands of revolutionaries would have been subject to life-threatening state repression.

It‘s debatable whether or not the government‘s shutdown of the internet was a hin-drance to the insurrectionary dynamic in Egypt. Some activists think that the shut-down advanced the process of the revolt, since without functioning cell phones people were forced to go out into the street in order to get news. This meant that the mood and conflicts were able to seize people without the mediation of the internet.

In short, if overloading is to be an effective tool of resistance against the cybernetic system-regulation, there has to be a critical mass whose communication is faster than the reactive censoring and counter-information. And it must succeed, or else the same infrastructure which allowed for a ‚revolutionary communication‘ will afterwards be transformed into a bloody instrument of repression against the then isolated ‚source‘ of the failed revolt.

Big Data Healthcare

Social physics and health policies

It is early evening as Bandar Antabi checks into his hotel in Munich. In one hour, he has to be at a business dinner at a restaurant he's never been to before. Before he gets there he has to have a telephone conference. The app of his data bracelet reminds him that he has done only 80% of the daily quota of movement. That is a reason for Antabi to be concerned. After taking his luggage to his room, he puts the address of the restaurant into his smartphone's navigation app. He puts on his Bluetooth headset and strolls on out into the sunset. While his smart phone's assistant maneuvers him through Munich's streets he dials the conference room. The participants have no clue about his little walk because noise suppression is filtering out all the background noise. The instructions for his navigation assistant stay unheard for his interlocutors – to them Antabi seems to be in an office. Shortly before he reaches the restaurant, his meeting is done, and as he takes a seat on the table, he fulfills his daily quota of movement.

What sounds like a near future scenario to most people is already reality in Bandar Antabis' life. The head of special projects of the Californian wearable-producer Jawbone is one of the people that has already taken the first step towards a new kind of connectivity. His data bracelet is the Jawbone Up24, the Bluetooth headsets Icon HD is also produced by Jawbone and is equipped with intelligent noise cancellation. The

voice assistant is Apple's Siri. None of these Technologies is spectacular on its own. It is the connection with each other and with data services in the background that makes them to one of the first examples what Antabi calls the „internet of you".

MEDICINAL CREDITWORTHINESS

Ages ago health insurances [in Germany] try to get a „detailed image" of our health. That incorporates all of our detectable habits of work, eating, leisure, shopping as well as other habits of our way of life and our personal tendencies. At the same time as the credit institutions' unlimited data hunger uses more than 80.000 (!) indicators to calculate our credit rating, the medicinal „credit rating" of each insured person is also being calculated.

These data do more than give statistical information about the correlation between health issues and an individual's life habits which may be responsible for those issues. They also make a detailed analysis of our individual risk of disease. In the future this data will be used to create completely individualized insurance options and dues.

The goal of this step-up „Evolution" is the subtlest possible categorization of risk. This is the highest refinement of the pigeon-holing that has been practiced by the insurance companies up till now. This indicates the complete undermining of the (first company-) health insurance fund's initial idea of solidarity.

Everything that we do and/or are unable to prove, or even things we don't do that we're not able to prove are counted into our credit evaluation. That sounds like the novel „*Zero*" by Marc Elsberg, which describes a global score that is a public ranking of all our efforts to improve our lives. Is it just a conceivable fiction? No, with all the insurance enterprises, it is very much a reality. For example the AOK [the biggest German health insurance company] uses the data analyst *Dacadoo* to evaluate a so-called „health score" for each and every member. The evaluation of the counted value is commercial secrecy. The processing operation is still declared to be „anonymous". This means that our individual health risks will be transformed into additional costs to be added onto a gradually shrinking basic care.

Not long ago, the Generali-group started to cooperate with the South African insurer *Discovery* to be the first ones in Europe to establish the procedure of telemonitoring for their life- and health insurances. Clients of Generali received premiums, vouchers, and in a second step more favorable provisions - if they were willing to verify their efforts to improve their health electronically. An app documents the preventive examinations such as screenings, step counting, and other sporting activities. The french Axa insurance is now going one step further. In an active co-ope-

ration with Facebook, it now adjusts its dues based on a systematic evaluation of entries in social networks. For three years the US-insurer United Healthcare has offered a discount if the insured person can verify that they took a certain amount of steps per day.

> ***If I am using my Payback-Card to buy cigarettes there can be very unpleasant questions asked by my health insurance - I should have chosen the cheaper, non-smoker rate.***

MEDICINAL CROWD FUNDING – THE INSTITUTIONALIZATION OF PITTANCE

Was does the future have in store for the people who will fall through the cracks created by a health insurance based on self-optimization and diminishing solidarity?

In the USA this is the bitter reality for millions of people: whoever cannot afford her/his medical expenses can present her/himself with their distress on online-begging-platforms. Come on, just apply for it. Tell the others why they should give their money to you and your operation. This represents self-entrepreneurship even in the case of illness. "Crowd funding" as the normalization of a casting process that is becoming more and more excessive. Conformists competing for favors from the „Gutmenschen", the „do-gooders". Who is allowed to live on and who isn't? The decisions of the internet community are based on a kind of scoring that follows simple rules. Who displays her/his need in the most heartbreaking way? This emotion-ranking is gradually replacing the health insurance's health score, which no longer has to feel responsible. The „crowd" that's taking part in this is allowed to feel like judges and lifesavers.

SCAN YOURSELF – BEHAVIORAL INFLUENCING AND DIGITAL SELF-OPTIMIZATION

How can I become fitter, happier, and more productive? They call them self „self-tracker", "life-hacker", or „qualified-self" movement. In 2007, long before words like „big data" existed, two geeks launched a website called *quantifiedself.com*. Though they started out as a small cult of self-proclaimed cyborgs that wanted to measure everything that was going on in or about their bodies, their practice quickly became a world wide trend. What is the purpose of this continuous quantification of as many characteristics of the bodily condition as possible? Is it self-awareness, self-improvement, even self-empowerment or more self-assurance?

The slogans span from „Know yourself, otherwise someone else will" to the fatalistic „Google, Facebook, etc. know about and record all my movements anyway, I want to at least have my share of the evaluations." At night, qualified-self-pros strap plastic strips around their head to record their brain waves. They measure their

blood sugar and body temperature, even if they are far from having diabetes or a flu.

Everything can be measured without any sense. A life contains how many giga byte? How much storage is used up by an affair, how much with a fight? Only a few of the many possible measurements of correlation make sense - but this is not the point. The being-trained-in the lust for measurement is posited as a learning objective and statement for the „not-yet-measured" people. It is about the imposition of a social principle: Find out your measurements/values! Verify your efforts! Motivate and discipline yourself! Bring us your data and we will help you in doing so!

SMART PHONE AS A CENTER FOR HEALTH

As patients and doctors [in Germany] struggle against the state-imposed functional organization of the electronic „health card" becoming a patient's digital file, Google and Apple simply ignore this conflict-laden negotiation process and let their smart phones become a whole center for fitness and health. For optimized health assistance "Google Fit" and Apple's "Health Kit" urge you to give them your lab tests and your doctor's statements. This includes your medication and your nutritional habits. Everything is included in a digital administration. In their „Green Book" on health services, the European Union reports that there are up to 97,000 different health apps. Despite their rich sensors, the smartphone lacks bodily proximity. For more reliable sensors that put their „fingers" on your pulse, there are a lot of so-called 'wearables' that communicate via Bluetooth with your smart phone.

24/7 RECORDING - BRACELETS AND SMARTWATCHES FOR UNINTERRUPTED TOTAL SURVEILLANCE.

SmartWatches, fitness-bracelets, and intelligent clothing (socks, t-shirts, and sports bras) log our heart rate, the calories we burn, sleep patterns, blood sugar, blood pressure and oxygen saturation without interruption.

The sensors of our constant companions are coming closer and closer to our bodies. The apps use a wireless connection to one of the many fitness bracelets or Smart Watches to count steps, measure calorie consumption, pulse, and blood glucose level - and they tell us how well we sleep. Whoever uses them will be able to determine whether or not they reached their self-imposed goals. No matter if it concerns weight loss, new top performances in sports, or just to live „healthier". In a playful and smart way a societal doctrine of self-discipline and -optimization is internalized. For modern top performers the hip fitness bracelets are already standard accessories of a functional lifestyle.

BIG DATA EXPLOITED - SPECIFIC INFLUENCE OF BEHAVIOR

The first insurance enterprises are offering cheaper options for people that can verify digitally that they walked more than 5000 steps a day. No problem for the paper boy or the minions of your local dog-walking start up. But a cashier will have difficulties fulfilling their walking quota. The Russian *Alfa Bank* gives out higher credits to their customers if the bracelet of their us-partner company *Jawbone* records that they care for their bodies in a disciplined way. „So healthy living can equal healthy finances, too", proclaims the producer of Jawbone. British based oil company BP encourages the exploitable self-monitoring, too, and blesses its employees with fitness-bracelets.

With the IT-supported and -controlled behavioral economics, highly efficient methods of social steering are created. The replacement of the fordist order (the „push" in the US-American management slang) for the exploitation of limited „freedom" („pull") has created new forms of social control. Yale professor Cass Sunstein introduced "nudging", which tries to get humans to do something without being ordered to do so. As if it were done entirely voluntarily. The guidance of Facebook-friends or the evaluation of the analysis-software is proven to be a more effective way to change your way of life.

VIRTUAL REALITY – MORE THAN JUST A COST REDUCTION

Anyone who still believed that the pioneering companies of the internet industries, Facebook in particular, are still limited to increasing their commercial revenues through the collection of data, through control and surveillance, was taught better after an interview with Zuckerberg concerning the purchase of *Oculus* in March 2014. Oculus was developed as a system of virtual reality for the gaming sector. After putting on the helmet, you are totally embedded in the world of the particular game. The frame of the screen is a reminder that reality has ceased to exist - the gamer is completely „inside". The game is the reality. The distance between the observer and the screen has disappeared. To the disappointment of Oculus gamers, Zuckerberg wants to take this as a starting point of a long term strategy to bring the internet mediated communications process to a whole new level. The connection between communication participants in virtual spaces shall shift the real communication processes that are happening face-to-face into virtual space. It is meant not only for gamers but also for the education sector and in particular for the health sector.

A patient or a student does not need to visit her/his doctor anymore, they „communicate" via Oculus-helmets. For the control of one's own movement in the „virtual consulting room", Oculus bought the hand-tracking-specialist *Nimble VR*

in December 2014. Taking the previous developments into consideration, this will have far-reaching consequences. The expropriation of face-to-face-communication in virtual reality gives more possibilities of control and even more for manipulation and conditioning alongside a gigantic potential for saving money. Equipped with cameras and sensors, the helmet permits the total control and view of the patient's surroundings. That includes detectable sensory data about their body and soul. In agreement with their objective of the total collection of data even in the emotional and socio-psychological sphere, Zuckerberg proclaims: "Games are only the beginning. After games, we're going to make Oculus a platform for many other experiences", so that it becomes „the most social platform ever". Zuckerberg stated that he „in doing so we will create the technology platforms of the future."

„Users can enter virtual realities to feel like they are together with loved ones around the world. Or they could feel like they are part of an event far far away." "Oculus has the possibilities […], to change the way we work, play and communicate completely." The Oculus-team instantly declared their enthusiasm for these visions on their blog. They proclaim the idea of a "deeper vision for creating a new platform for interaction that makes it possible to connect a billion people in a way that was never known by now."

It becomes immediately clear that by integrating various modes of expression, these projects want to usurp the control humans have over their feelings and histories ("timelines", "stories") to an extent not yet before seen. Google and Apple want to follow along.

GIVE US YOUR DNA – THE MAXIMUM POSSIBLE ACQUISITION OF DATA

Carried by the „power of hope" Google wants to push the very the lucrative transition from an analogous to a fully digitalized society forward, especially in the field of medicine. Stem cells, custom-made cancer treatment, genome analysis, gene therapy, and nanomedicine are parts of Google's own experimental laboratory. To continue on where medicine and science have reached their limits. With their market power they have created something that three generations of Nobel Prize winners weren't able to do: to recognize health as the management of information about our bodies.

Whoever discovers the cancer early enough, whoever influences the aging processes at the right time and whoever lives her/his life in a supposedly perfect way without the fear of regrets has to be able to distinguish their body from its realization in the digital grasp.

The economic benefits: with the ethic of healing, Google can hope to polish up its damaged reputation of being a Big-Data-business' limelight addict. The can-

cer screening-bracelet, which was at first seen as a peculiar innovation of Google‘s microbiology division, could provide google’s image with a quantum leap in less than than five years. By injecting magnetized nanoparticles into the body that constantly follow the bloodstream, the bracelets’ magnetic sensor is monitors the appearance of cancer cells in the body 24/7.

With the collection and decryption of the human genome, Google tries to gain supremacy through data. With the access software for genome data, presented in June 2014, Google presented the most important platform for its „Google Genomics“ project. From now on, the Google Cloud is in charge of the analysis and exchange of data between the worlds’ two biggest genome databases.

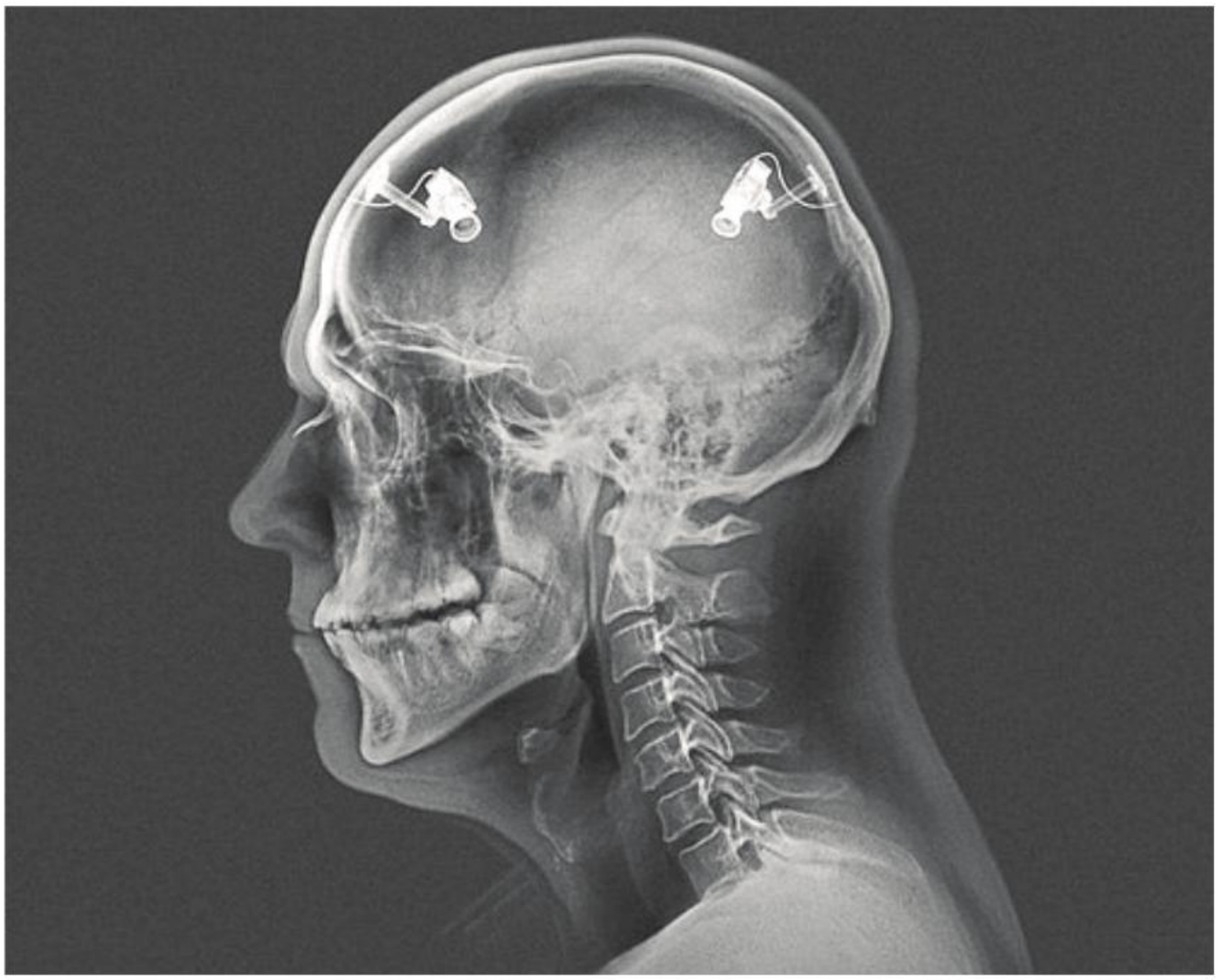
To give the „genome revolution“ a leg up, apologists of techno-progress like the Walldorf-based software company SAP cooperate with the whole process. They are pushing for their 65.000 employees to have molecular profiling in order to enable custom-made cancer treatment. The costs for the genome sequencing (only about 1000 Euro per person by now) is covered by SAP. Through a foundation established by SAP-founder Dietmar Hopp, other people are expected to give access to their genome information as well.

Therefore the re-measurement of the basic codes of human life is intended to pickup speed. The protagonists of the process pretend to be confident that this is a winning ticket:

> ***„We have begun, nothing will stop the progress“, says Craig Venter, genome-project pioneer.***

Health as a system in digitalized capitalism

To withdraw from the digital colonization of our bodies



The German electronic health-card(eGK) is one of the biggest IT projects since after the war. Since 2006 it has tried to implement a comprehensive coverage with the eGK - nine years, millions of people and free minded doctors oppose the project. The health benefits that accompany the usage of an electronic card are not evident to them. The relationship of trust between doctors and patients is being jeopardized, since sensitive health information is taken out of the doctor's office and stored in a centralized Cloud. At least 2 million employees of the health industries have access to it, leaving the possibility of unauthorized access. There are unlimited possibilities for the use of our sensitive health information.

THE HEALTH BUSINESS

In 2001, the consulting firm Roland Berger proposed the chip card. Two years later the Federal Ministry of Health got the project consortium bIT4health - (better IT for better health) involved. The participants are IBM Germany, Fraunhofer-Institut für Arbeitswirtschaft und Organisation, SAP Germany, der InterComponentWare, and the ORGA Card Systems (now Sagem Orga,). There goal is it to define the se-

curity infrastructure and the telematics' framework architecture. Until now planning costs have risen from one billion to nearly 5 billion in only five years. Another increase of costs is expected - up to 14 billions. Who is earning from this?

The eGK and the telematic infrastructure - that is the entire system with all its abilities and functions in the Cloud, concentrated in 8 to 10 data centers. In the meantime there is a specialist for the boundless evaluation of very sensitive personal data: the Cloud4health consortium which is made up telematics of the Averbis GmbH (a specialized software company), the Rhön-Klinikum AG (a leading private hospital group in Germany), the Fraunhofer Institut SCAI (Fraunhofer Institute for Algorithms and Scientific Computing), and the Friedrich-Alexander-University of Erlangen. In August 2014 in a Berlin wine bar a new lobby group was founded by a very select group: the Association for Digital Health (Verband digitale Gesundheit, VdigG). It a an association for the „determination, discussion, representation, and communication of the chances of digital hard- and software solutions, as well as networking solutions for the health sector." We are delighted that they put thought into the material optimization of health care.

Arvato - a Bertelsmann subsidiary is already running the teleformatic infrastructure. Telematics originates from „telecommunications" and the „informatics" which connects medical practices, pharmacies, hospitals, and health insurances. This subsidiary is setting up data centers for the eGK as well. The impact of the eGK can only be understood on the level of teleformatic infrastructure. It first paves the way for an evaluation of everybody's health information. A biological pool of information is created that promises not only to bring in huge profits but also to open the floodgates to manipulation.

Among other things the „Stop-the-E-Card"-campaign criticized that one Arvato subsidiary, the AT Direkt, is the biggest vendors of addresses. Furthermore they claimed that the Arvato Infoscore provides services for financial information and credit reports for debt collection agencies. Telekom, the biggest German telecommunications provider, has founded the Telekom Healthcare. Even companies that had no connection to the healthcare sector were profiting from this new line of business.

„Stop-the-E-Card" criticizes that via E-Card and teleformatic infrastructure, sensitive health information can be saved onto a centralized data storage unit. This further consolidates the neoliberal approach to public health and encourages the interests of the health care industry. The E-Health-Law announced by the German Ministry of Health (originally for October 2014) would accelerate this development further. This law has yet to be passed.

SPEED, SPEED, SPEED - THE NEW SPORTS CAR WANTS TO BE TAKEN OUT FOR A SPIN

Since the beginning of 2015 German minister for health Hermann Gröhe has become increasingly belligerent in revealing his concept of health, technology, and patriarchy by comparing the eGK with a sports car that wants to be taken out for a spin. He says that we finally need „Datenautobahnen" - information superhighways. From his point of view, digitalization is an inevitable part of our future. The central argument that Gröhe has presented to the public is that the use of electronic emergency data could be used by any doctor, and could thereby save lives. Gröhe wants to speed up this process. People who try to block it from happening will be punished, and the fines are getting more and more expensive.

The following January a draft bill of the Electronic-Health-Law was welcomed by Bitkom, the IT-industry's lobby group. They called for the process to be sped up and for tougher sanctions in the enforcement of the teleformatic infrastructure. Those who advocate the health-card yet are concerned with keeping their data private have requested a protection against the confiscation of medical information by the data processing industry. Physicians criticize the law draft as being a compulsory enforcement of data exposure. They are sure that this will not improve the quality of treatment.

After the revelations of Snowden and others, we know that there is no protection from the misuse of data. No law will change that. The only given consequence can be the prevention of data pooling and that sensitive health information be made available exclusively or individual use. Or, to put it in juridical terms: informational self-determination. The act is planned to be enforced on January 1st, 2016. By 2018, it will be followed up with another repressive plan.

At a „Freedom not Fear" demonstration in August 2014, a representative of the medical faculty spoke about the impact of the electronic health-card. He raised questions concerning the card's enforcement:

„Who has which disease and what kind of health issue? Who takes what kind of medication? Who is suitable as a consumer, as target group for the interests of the pharmaceutical industry, the industries of health care and other health business? Who constitutes a risk and is therefore not given life- or invalidity- insurance? Who will be refused health insurance, a loan, or maybe even a job?"

The insurer, the information technology industries, and the so-called health sector are the parties interested in this project. Within this context, informational self-determination no longer exists. There is a strong likelihood that our sensitive health information will be used to manipulate us, extort us, even to ostracize us. In

Germany, as in other countries, it is legal to sell data - if it is anonymized. All the experts guarantee that with the central storage of our data, their re-personalizing would be possible. The project developers know that depersonalized data can easily be re-linked to people through metadata. The technical term for it is „re-engineering“. The job interview went well, but you didn't get the job. The company had information on a so called hereditary defect. You have not yet been limited by it and maybe never will be, but there is information about it. This piece of information has let to a negative decision.

Informational self-determination and the central pooling of medical information are mutually exclusive.

THE SELF-OPTIMIZATION OF OUR BODIES

“Based on our guidelines and the consensus regarding defined standards of healthcare, this program is being used to observe symptoms, and patients' self-reliant actions are supported. They are being informed and guided. The data logged by the therapy-management-programs provides information on the use of resources in care, patients' satisfaction, the quality of life and patients' compliance.” From the Bosch Telemedicine System‘s web page. What does a provider want to tell me with such a statement? That it is all about my (customer-) satisfaction? That a piece of technological equipment will explain to me what self-reliant action means? That my health will be managed. By whom? Am I a lining part of this process or a machine yet? The media is full of stories of so called life-optimizers like SmartWatches. The health business is booming The fitness-tracker monitors the amount of steps we take or our movements during the night, transmitters in a chest belt permanently measure our heart rate, a machine reminds me to take my pills, Cardio Dock is plugged into my blood pressure meter and records data on me. The growing market of mobile health appliances is enormous. It is referred to as mHealth – mobile health. In 2013 6.6 billion dollars were spend on mHealth and market research companies predict a business volume of 20 billion dollars for 2018. There are more numbers of this kind than you want to read about. What is happening now is quite simple, really. There is a nearly uncountable amount of data being collected. They are used to develop algorithms that bring general statements into the world (see“-Big Data Healthcare“ in this volume.).

TREATING MENTAL DISEASES WITH APPS

Other apps that will improve the diagnosis of mental diseases are also being praised. For example evaluating the severity of a person's depression by analyzing their patterns of motion: how often is the person moving, how many people are contacted by phone, how many text messages is the person writing? The more in-

formation gathered, the more distinguished the diagnosis, the algorithm that is developed. And if I just want to be on my own, without any communication, does that make me suspicious-looking? Is „everything OK" with me, are any indications of a mental disease? The fact is that the entirety of daily life is being monitored and the data being stored: how I move, what I eat, how long I sleep, how I communicate, how I feel... At field of psycho-informatics at the University of Bonn apps are being developed that are designed to monitor people with depression disorders, especially their social behavior. The University of Michigan developed a voice analysis program that will be able to diagnose post-traumatic stress disorder, schizophrenia, and Parkinsons. The EU sponsored project Monarca supports the use of smart phones in the monitoring of bipolar disorders. The list goes on.... Scientists are thrilled by the magnificent possibilities of control given to therapists or to the patients themselves. The amount of sensitive data collected is not a problem. The internet companies already have a lot of sensitive data, because we give it to them voluntarily. Surveillance secures submission and the collection of data creates people that are accessible as well as controllable. And if you don't want to take part, you will be excluded, outcasted, isolated. There is one rule in rankings: the only thing worse than a shitty rating is having no rating at all. This ensures that you play by the rules.

THE PATRIARCHAL LOGIC OF THE IT-WORLD AND THE ALTERNATIVES

If I want step out of the world of dead machine logic, I have to leave the logic of modern natural sciences that are part of the information technologies The dominance of the visible leads to a reduced role of the human in this field. It also means the exclusion of haptic methods (methods that relate or are based on touch) and other methods of alternative medicine that work outside of the natural sciences. Experiences of touch and smell are more or less non-existent. The alienation of our own body, of our feelings is very sophisticated. All that is living seems to be frightening, has to be controlled. The modern human is not a body anymore, it just has one. For digital economics (of which mHealth is a part) life processes are just the sum of physical-chemical processes.

For example ultrasound: The feeling of being pregnant has to do with making it visible, with a technical procedure. Happiness is created by viewing sonograms. It is a procedure that expropriates corporeality. My body and my feelings can only be experienced by technical mediation, by a device that produces certain pictures that I first have to learn to understand or that have to be explained to me. This blocks the access to myself and makes me dependent on specialists. Reducing human beings and their diseases to imaging techniques (ultrasound, MRT, X-Ray, CT) produces a specific kind of disease that excludes everything that cannot be seen and therefore disregards it. Feelings and pain are non-representable but are a genuine part

of human existence. Where should they go? Self-perception and self-competence are becoming terms we no longer understand. Being separated from myself, my body and the exclusive mediation to my body by means of technology may lead to a situation in which humans will be manipulated and controlled by a very lucrative technology. Man vanishes in the machine. This technology reaches a different dimension than the one of railroads and automobiles. Technology as a devitalized economy is a tool to make social machines of us all.

From a feminist perspective digital economy is a violent, patriarchal technology realizing the principle of optimization and (subsequently) of exclusion that destroys the social.

It is a „modern" form of Social Darwinism demanding that we be "permanently fit". According to this logic, disease is self-inflicted. Propaganda tells us that nobody will get sick if everybody does what the apps tell them. Whatever we do it always our fault and we have to pay. That is another argument for abandoning the apps.

Health is really about our body, our mind and our feelings, all of which cannot be found in the discussion by eGK. Where have they gone? The only concern is the availability and collection of our sensitive health data. Acceleration and centralization are two categories that are more associated with disease than with the health. As the numbers of those suffering from depression and so-called burn-outs show, our every day life is digitalized ever faster, making lots of people sick. We have less and less idle time, even sleep should be optimized. The digitalization of the health care system intensifies this development and optimization always excludes those that cannot or do not want to keep up with it.

At the time being (2015) the card has only the same functions as the old one - with the addition of a picture of the owner. But that will change. Everyone should discuss with her/his doctor to find ways to resist the data in the cloud. Whoever doesn't have a eGK or „loses" it, can get a „paper-based proof of entitlement" issued by the health insurance.

If we submit to the incentive of self-optimization we invest in their desire of permanent involvement and productivity. Let's reject this process and its acceleration! Let's live an unpredictable life. We will not let them steal the knowledge of our bodies and sociability. To withdraw from the digital colonization of our bodies. Let's build the digital-free alternatives and attack their interface circuits.

Self-organization on open platforms

WHY THE SHARECONOMY IS NOT A PROGRESSIVE ALTERNATIVE

Wikipedia is considered to be a positive example (with limitations) of the democratization of knowledge in the course of the digital integration of our lives. It is not an encyclopedia like the Encyclopædia Britannica, which regulates access to knowledge, how knowledge is selected and compiled. Instead, the „encyclopedia's" user community collectively negotiates about which content is displayed in which way. In the best case scenario the platform's organizers take the back seat, merely moderating the process of knowledge aggregation according to transparent rules. So far, so good.

The more digitalization proceeds, the more access to music, movies, rental cars, ride sharing, holiday accommodation, co-working spaces and everything one can „share" is organized over platforms. The shareconomy is spreading to more and more areas of life. Leftists often interpret the decline of hierarchical organizational principles in conventional institutions as a chance for emancipated (self-) organization on „independent" platforms. Some even see this development as a paradigm shift that will sooner or later replace the capitalist market organization with a cooperative community economy. That sounds good. But how does it fit together with the current concentration of power by global „service providers" such as Google ? Not at all!

OLD SCHOOL MARKET CONCENTRATION - FORCING OR BUYING OUT

After Bell invented the telephone in 1876, the world's first telephone company AT&T (American Telephone and Telegraph Company) was founded. Starting in the 1920's overhead power lines and telephone cables were being lain in US cities. Initially AT&T was not interested in rural areas. Due to the low population density

and the small number of households that were to be connected, the investment costs were deemed to be too high.

Since the villages wanted to be able to make phone calls, numerous local initiatives were founded that laid telephone wires independently. By and by these „cooperatives“ became growing, local telephone providers. After fully connecting the areas of high population density, AT&T no longer wanted to tolerate the competition of the 'cooperatives'. They tried to either trick them out of the market or buy them out. The aggressor of the economic war that ensued could be sure the arbitrator, the Federal Communications Commission, would intervene on its behalf: the small providers were forced to cooperate with AT&T „for the benefit of the community“. Consequently this meant their absorption by AT&T.

This economic war during the pioneering days of telecommunication tells us almost everything we need to know if we want to understand why it is relevant that progressive and decentralized sharing concepts are being eliminated on growing internet platforms.

EVERYTHING WILL BE A PLATFORM - THE ELIMINATION OF CONVENTIONAL INSTITUTIONS

Today the internet is connecting more and more people, databases & the services based on them and objects & the procedures for controlling them. The result is a crisis for the conventional institutions that are responsible for managing these objects/data. In many cases they've already become redundant. Who needs a taxi dispatch when a ride-hail app can be used at anytime by anybody wit a smartphone? Holiday housing providers are replaced by the Airbnb app, ticket counters are replaced by their websites and apps. And classical institutions such as clubs and other places where people meet face to face are being replaced by social networks on Facebook. In what follows, we won't take the reliability of the services offered into account.

Platforms and conventional institutions share the task of gathering people, interests or knowledge so that they can be exchanged mutually. Conventional institutions control this in a centralized way, on internet platforms do so in a decentralized way via "peer to peer". Platforms like Facebook have centralized data centers but the contact to others is organized autonomously and in a decentralized way. In contrast, the conventional institution of a taxi dispatch does not intend to provide callers with autonomous and direct contact to a particular taxi.

It is indeed conceivable that the crisis of conventional institutions, especially those relevant for regulatory policies, has created a welcomed loss of control capable of undermining conventional forms of organization. Hierarchical organizing prin-

ciples could be replaced by non-hierarchical platforms with direct „end-to-end“ exchange.

This all sounds wonderful. However it ignores the fact that the social processes happening on platforms don't take place in a power vacuum– they too are subject to capitalism's valorization process. The administrative regime called into question will be replaced by a new one. New players like Google, Facebook, Amazon and Apple determine the rules for what their platforms „offer“ and in doing so, as multinational, non-state actors, they even defy conventional political negotiation processes. The dynamics of this new order are driven by maximizing the collection of data to control those who contribute this data. It therefore offers absolutely no potential to organize society decentrally and autonomously. The goal of having plenty of data and using self-learning sets of mathematical instructions (algorithms) to analyze it allows for a concentration of power and the subsequent shaping of a future society to an extent never before seen. The platform as a generic, decentral principle of organization turns out to be the ideal means to centralize observation and control.

Through a mish-mash of new-age-utopias and bizarre dreams of the self-determined American individual fueled by sparkling start-ups & an ultra-capitalist culture, a „Californian ideology“ was taking shape.

SHARECONOMY – BENEFICIARY OF PLATFORMIFICATION

Property does not vanish but becomes increasingly less important for the use of some goods. Digital media can be copied for free, movies, music and (e-)books are downloaded instead of purchased. Usually people pay flat-rates, a monthly fee that allows them to download as many different media as they want. If this is done legally, the user is often just purchasing a license to use these digital media under certain conditions, similar to borrowing media from a conventional library.

This way of using things can be extended to goods that cannot be copied digitally. Sharing a car with many others was a reasonable concept even before the interconnection of the world via information. But only with permanent access to the „quasi free“ administrative infrastructure of car-sharing-platforms on the internet does sharing becomes cheap and comfortable enough. Who the car, the flat or the desk in a shared office belongs to is no longer an issue if you want to use them. It is even easier to share goods that don't need to be maintained or taken care of, such as shared parking: by now private parking spaces can be rent out by the hour. Booking and paying are fully automated with a simple smartphone app.

In a few years time, the „Internet of Things“ will connect almost every item with the internet. In doing so, it will allow itself to be contacted by other items and users, which will further promote the „shared“ possibilities of using the shareconomy. The promising „sharing“ of goods does not challenge ownership since the “sharing” it advocates doesn’t imply that the common use of public goods is free and non-commercial. Generally they are not (in the long term). And there is a powerful reason for this.

THE NETWORK EFFECT - CENTRALIZATION INEVITABLE

The most important reason for the growth of platforms are so called network effects. „We“ are on Facebook because everyone is on Facebook. „We“ buy on Amazon because they seem to have everything. „We“ use android or iPhones because lots of apps are available there. The network effect describes how the bigger a network is, the more participants begin to use it. It gets stronger and stronger the more people, datasets, apps, products and developers are absorbed. Finding appropriate friends, life or commercial partners on platforms like Facebook, E-Dating, Ebay or Amazon follows this simple rule.

The utility for the users rises with the number of (totally registered) users/products according to the amount of possible direct „end-to-end“ connections of participants. The utility also increases for the providers since they sell the data they collect to analysts. Therefore a consolidation process from lots of small, specific forums to a few big networks is the natural consequence.

This network effect was already a decisive component of the American telephone company AT&T’s forced growth. Yet while there are limits to the growth of conventional networks (e. g. service networks) there are none for platforms once the network infrastructure has been created. For platforms on the internet, communication is the most important commodity. It can circulate unhindered by geographical factors. In contrast to previous markets, platforms do not differentiate themselves geographically but functionally, thematically or with fixed identities. The tendency towards monopolization forced by the network effect is opposed only marginally by individual groups of users who switch to alternative platforms to differentiate themselves from the rest of the world.

Google even profits from the way different platforms mutually intensify each other’s effects. The heart of it all, Google search, intensifies the network of connections between single databases for the world market leaders providing internet browsers (Google Chrome), software for mobile devices (Android), online videos (Youtube) and mail providers (GoogleMail) .

The „datafication“ so forcefully promoted by Google will further increase the effect this has on the Internet of Things. Recent acquisitions of companies producing thermostats, smoke detectors, household robots, surveillance cameras, driverless cars, satellites, drones, internet undersea cables and internet balloons suit the purpose of placing their own system software „virtually everywhere“. In doing so, they guarantee their access to the largest possible portion of the worldwide data infrastructure. This standardization of different platforms gives them access to each other's users.

The *"winner takes it all"* monopolization is far more likely to be the future of platforms than Jeremy Rifkin's „collaborative communities“ utopia. The rapid rise of present shareconomy protagonists Airbnb (accommodation) and Uber (Taxi) proves that. However for the platforms that deliberately began openly and independently, the following is true:

COMMUNITY-EXPLOIT: USE AND DEVELOPMENT STARTS OPEN & ENDS CLOSED

The short history of Twitter reveals this phenomenon: In the beginning, Twitter was a platform run by the community of users. Later, it was closed down and used commercially.

Twitter started as an open infrastructure. Tweets from different sources could be configured individually and compiled into an individual stream of messages. Since the program interfaces offered by Twitter were open to everyone, even the software necessary could be developed freely by the community. That's how lots of different Twitter clients (software for the individual use of Twitter) became available for all operating systems. The community of users rapidly increased to about 1.5 billion members.

In 2008 Twitter bought Summize, which offers a multiplicity of search options on Twitter. In 2010 it bought Tweety, the most successful Twitter-app for Apple's iPhone and iPad. Access to programming interfaces was regulated and in 2012 it was more or less closed. In 2013 the possibility of using Twitter anonymously was shut down and thereby the access to billions of tweets was strongly limited. Since then, Twitter users are not allowed to determine the sources of their messages by themselves. That's how Twitter's business model as a background service, so praised at its inception, was able to be adjusted to the business models of Google in Facebook in the course of just a few years: *closed development and registered use to collect user's data and exert influence over them at the same time.*

Google and Facebook are buying successful start-ups by the dozens. Most recently in January 2015 Facebook bought the open development platform wit.ai, on which

more than 6,000 developers have been programming self-organized speech recognition software for years.

Peter Thiel, one of Silicon Valley's most radical masterminds, calls his advice to executive consultants a strategy of creative monopolies:

> ***"Choose a market that you can dominate, build a monopoly and try to keep it as long as you can."***

A free software project is unfortunately no guarantee for an independent solution in the medium term. The better the idea, the higher the chance it has of being bought, replaced or infiltrated. Wikipedia also has to deal with this situation. Pressure needs to be applied by involving a community of hackers, just as *Tor* has managed to remain independent on a long term basis despite numerous offers and attempts to infiltrate it.

War on Cash

The EU wants to abolish cash

The EU commission wants to eliminate the only anonymous means of payment available to everybody: cash. In the future, our financial transactions will be handled exclusively through cards, accounts, and smartphones, all of which are electronically traceable and attributable to specific people. The commission's intended program of stimulating consumption via negative interest rates will only be effective if cash is more or less abolished. Otherwise, it would be possible to hoard money at home to protect it from the negative interest rates.

We all know the incentives to give up cash: in many cases, you would only be able to claim a bill for a craftsman as a tax write off if the payment is made by a bank transfer. In some major cities' public transport systems, rebates are offered if people pay with card. But now things are getting serious.

In Denmark, by 2016 gas stations, restaurants and small stores won't be required to accept cash anymore! The Danish central bank wants to stop printing cash by the end of 2016. Other Scandanavian countries want to follow this plan. At the moment in most other european countries, a cap on cash payments is in place. In Germany, there is discussion of making a 5,000 euro limit to cash payments. Since September 2015 in France, it has been forbidden to pay cash for anything that costs more than 1,000 euros. In Italy that's been the law for a long time. The forerunner is the Troika-dominated Greece, where the cap on cash payments has already been lowered to 500 euros. In the ‚negotiations' with the financiers, there is discussion of a 70 euro limit - the virtual elimination– of cash.

The EU- commission wants to herald in the end of the only *anonymous* means of payment available to everybody. In the future, our financial transactions will be handled exclusively through accounts, cards, and smartphones. As a first step, the 500 euro bill will be permanently removed from circulation in the entire Eurozone. It is already forbidden to carry more that 10,000 euros cash when crossing European borders.

IT'S ABOUT CONTROL– AND PROFIT

The main argument for the abolition of cash is– surprise surprise– ‚*security*': by opening people's accounts, it could be proved that they worked illegally, tax fraud would become more difficult and fighting organized crime would become easier. There would also be less bank robberies. „*The blood in the veins of criminality*", that's how Stockholm's police president describes cash.

There is an economic reason for abolishing cash. Since the euro-crisis, the European central bank doesn't ensure monetary stability, but rather tries to actively stimulate the economy by fixing interest rates. Their desired mode of action: they want to force us to consume. Since the money on your account doesn't bear interest anymore, but rather diminishes due to negative interest rates, you will want to spend your money immediately rather than let it sit in your account.

For seven years now, the central banks have practically eliminated interest rates. In addition to that, they pumped 10 billion euros of fresh cash from the printing press into the economy to preserve the illusion of having a functioning economy. But that was not enough, hence negative interest rates were the next ‚logical' step. *Kenneth Rogoff*, the former chief economist of the IMF said

> ***„Cash is the decisive impediment to lowering the central bank's interest rates even more."***

According to his point of view, if we had no cash during the height of the financial crisis, 4 to 5% negative interest rates could have been implemented. That means we would have paid the bank for our cash. But as long as customers are able to withdraw cash and stash it at home, the burden of this negative interest rate can't be handed down to the customer.

And supposedly, there's another reason to abolish cash: hygiene. Europe-wide, around 57 percent of people found bank notes and coins are among the most unhygienic objects, says a 2013 study from Mastercard.

CASH HAS MANY ENEMIES:

- Many big retailers hate cash. It has to be guarded, counted and in the evenings it has to be delivered to banks in strongboxes. Big chains want to set a custom price according to the customer's habits of consumption and the time of year in which products are bought (for example, chocolate would become more expensive around Easter time). However on a grand scale this would only be possible without cash. In non-digital commerce, dynamic prices are

only attractive if the retailers have a very exact knowledge of their customers' preferences. And flea markets, those pesky competitors in the low price range, wouldn't exist without cash either.

- The banks– no cash means no bank robberies; and cash machines are too expensive to maintain. More importantly: without cash everybody would be economically depended on the bank, which can lock our cards at any time. And when the bank is broke, so are we. As a result, banks would once again be what they were during the financial crisis: indispensable, unassailable, since with their end would entail the end of all economic life.

- The state– without cash, there would be no illegal work, and the economically transparent citizen would finally become a reality. Secret services, intelligence agencies and police will only be able to obtain this transparency via the electronic traceability of every financial transaction without cash.

- Those who profit from the digitalization of our lives– from Amazon, Apple, Google, Facebook, Snapchat, Paypal / Ebay all the way up to the clever start-ups. They earn money when we pay, debit, and change our booking electronically. For them, an exclusively digital payment would be a wet dream. The Ebay daughter Paypal obtains significantly more information about its customers: when not only the auctioned bicycle, but also the morning coffee and evening visit to a restaurant are handled by the payment platform. The service receives commission for every transaction– between 1.5 and 1.9 percent of the price, plus 35 cents according to some statements. For retailers, that can definitely be cheaper than the 2 to 4% that are ordinarily charged for credit card payment. *Apple Pay, Google Wallet*, as well as the newest drafts of Snapchat and Facebook and many other retail chains make it possible to transfer money via smartphone– entirely without banks– yet completely personalized.

- Health insurances and other insurance companies want to track if we eat fat and unhealthy foods, smoke, or take other individual risks that are quantifiable via Big-Data. Based on this data, we will be assigned personalized dues.

- Data gatherers and analysts like Google's financial service provider Zest strive towards a complete portrayal of each individual. This portrayal could then be sold on to other companies. For Zest the top-class of the big data concerns „all data are credit data". With over 80,000 indicators, it evaluates the credit-worthiness (our score) of everybody that uses the internet worldwide. The transactions we make in the supermarket provide data about our consumption habits, bank transfers provide information about our social milieu. Thanks to the connection of data regarding payment and location, other sources of

personal information (search engines, Facebook, mail, chat) and promotional networks, behavior control can be customized *outside of the internet* as well– for example on screens in the supermarket or via smartphone messages.

CASH IS KING IN GERMANY – STILL!

„Only old people and bank robbers still want cash today".

With this slogan, the unions, banks, and retail chains took a stand for the complete abolition of cash. In Scandinavia and the USA cashless methods of payment are far more widespread than in Germany.

In contrast cash is used for almost 80 percent of transactions in Germany, and almost always for small transactions. If one considers the volume of transactions, only 53 percent of the entire value of goods and services in Germany are paid for with coins and cash. The percentage of „Giral Money" – money that is moved via bank accounts with checks, transfers and cards, or with Paypal– grows constantly. EC cards have superseded cash as the favored method of payment for transactions between 50 and 100 euros.

Mobile payment, however, is still in its infancy. According to the German Central Bank only 2 percent of payments are settled with cell phones. Yet this year the big retail chains Aldi, Metro, Rewe and Kaisers want to offer mobile payment options for modern smart phones that use contact-less near field communications (NFC). A matching wallet app for the respective service provider will then have to be installed on the smart phone.

Especially with Apple's new smartphone payment system, a drastic change is to be excepted. At the time being, *Apple Pay* exists in the US and in England. Apple collects 0.15% of every transaction. Google also wants to push its way into this market, even though there are difficulties in starting: with its payment service, Google also wants to generate key words for online-advertisements. But at the moment, only a few banks and retailers voluntarily share their data and all follow up transactions with Google. Google can earn more money by customized advertising and by charging a couple cent fee for every transaction.

PAYBACK POINTS AS A CATALYST FOR THE TRANSITION.

Since the money-conservative population of Germany is still not very open minded about the new payment technologies, other incentives are needed to break out of the traditional ways of payment: payback points. These are for all the bargain hunters willing to reveal their consumer behavior over the modern version of the

loyalty card for just a few points.

But what would happen if the information we make readily available turned against us? What if, after the successful gathering of payback points, instead of that much desired pepper grinder waiting for us, our health insurance raised our dues. Because it would be discernible that the payback card was used to buy cigarettes many times during the week even though you claimed to be a non-smoker?

BITCOINS– VIRTUAL MONEY AS AN „ANONYMOUS" CASH-ALTERNATIVE?

Since every transaction made with credit cards, EC cards or cash cards is permanently saved, in 2009 programmers developed an alternative method of payment: a currency called *Bitcoin*. Established through open source software, the Bitcoin network creates the possibility of making bank transfers under pseudonyms without the regulation of central authorities.

How can I pay with Bitcoins? You have to install a program on your computer or smartphone that manages the currency. For example *Mutlibit, Electrum,* or *Armory*. You are not required to give any personal information when opening an account.

The program generates a file called Wallet. It also creates one public and one secret key. The public key functions like an account number as an address and looks something like this: 1EQodj2MkD6iL5X4MZ7Pc6kWMArF7moW6E. The user gives this key to the people s/he wants to trade with or to people from whom s/he wants to receive Bitcoins. However the secret key is best kept to the user, since it can be used to identify him/herself in the Bitcoin network. The secret key is needed to be able to send Bitcoins. It‘s as easy as online banking. However if the secret key is tracked, the account can be emptied out. For Bitcoins, you can‘t cancel transactions– once made, they are irrevocable. There‘s no bank you can turn to. If you want to use Bitcoins, you have to keep your key safe and use it carefully.

Principally, Bitcoin is built upon internet anonymity. For private persons and businesses, transactions aren‘t traceable unless more information is given. Provided that neither the IP address nor the Bitcoin address can be attributed to a person, the protection of private information offered by Bitcoin is far better than that offered by payment methods that use accounts, cards, or smartphones.

The anonymity afforded by Bitcoin is nevertheless restricted and offers no protection against the methods of persecution used by intelligence agencies. In this case, the user must use the especially secure Live-operating system like Tails to ensure anonymous internet access. Furthermore, it must be kept in mind that for transactions

between businesses, at least one side must partially compromise their anonymity. All transactions between two addresses are logged publicly, constantly updated and saved permanently in the Bitcoin network (decentralized and ten thousand fold). If a connection is made to a person at any point, for example through an intercepted consignment of goods or service provided, all the transactions attributed to that address can be traced back. Thus there are more opportunities to track transactions than there are when using cash.

One of the main advantages of using Bitcoin accounts instead of classical bank accounts is that no government agency can freeze the funds received in Bitcoin accounts.

The service that enable the conversion of Bitcoins into other currencies are normally subject to the regulations put in place to fight money laundering. For example they don't see themselves as being obliged to unfreeze money that might „possibly have been acquired illegally." For more on this, see „mtgox.com has blocked my account with 45 000 USD in it!", „Complaint" of the user Baron as well as Mt.Gox's response are on bitcointalk.org, November 21st 2011.

In addition, Bitcoins can be preserved on an encrypted data carrier. Watch out! If you forget your password, the money on the account is also lost– just like with cash.

The protection against counterfeit, i.e. the guarantee that nobody else can spend my Bitcoins, relies on a cryptographic procedure that has yet to be cracked. This ensures that your private key cannot be reckoned from your public key, which is available for all. The repeated use of the same Bitcoins is prevented by the so-called ‚*Proof-of-Work*' procedure. In order to counterfeit a ‚Proof-of-Work', an attacker would need to have access to more computing time than all honest Bitcoin users combined. This condition can only protect us from offices like the NSA in the long term if a very large number of users join the network.

The difficulty up until now has been monetary stability: the exchange rate during the conversion of Bitcoins into a ‚central' currency. In the past few years, the value of the virtual currency on world-wide Bitcoin trading platforms has been a roller-coaster ride. Additionally, access to Bitcoins is strongly restricted in some countries, such as Russia and China.

Stellar Coins represent a new species of Bitcoins. The new crypto-currency is very similar to Bitcoin. However, in contrast to Bitcoin, it is managed by the Stellar Development foundation. For this reason more transparent than Bitcoin while at the same time maintaining the same degree of independence offered by Bitcoin. The goal is that every person in the world that has access to a smartphone or a compu-

ter will be able to send money to any person in a matter of seconds– without fines and without profit.

„FINTECH"-BRANCHES ‚ATTACK' THE CLASSICAL WAY OF BANKING.

Some technology companies offer alternatives to the financial institutions' partially overpriced services, thereby gnawing away at their profit. Paypal offers easy money transfers, you can open a completely mobile checking account with Number 26 and you can send money to foreign countries at a very low cost with Transferwise. The finance-technology companies such as Iwoca allocate credit to independent and small businesses for six months at an interest rate of 2% per month. In doing so, Iwoca advertises the ability to make lending decisions within one day. The borrower undergoes a credit check steered by an algorithm that includes classic scoring-results as well as information made available from social media. Whoever doesn't reveal themselves on the internet receives poor loan conditions.

Just like the entire Silicon-Valley startup scene, the Fintech-branch is growing rapidly: in 2014, the amount to be invested in the industry grew from 4 to 12 billion dollars (compared with the year before). Some classical financial institutions try to earn money with this business by purchasing shares of small, aspiring technology start ups.

DEFEND CASH!

Recently, advocates of both data protection and user protection have gotten together to form the first initiatives to defend cash. For them, it's clear that cash is an essential piece of ‚citizen liberty'. Without cash, state reconnaissance and user manipulation would reach a new level. Additionally, they doubt that abolishing cash would be economically beneficial for a given country: the majority of studies that try to prove that digital payment systems are all-around ‚cheaper' than cash come from credit card companies.

Why should we, as opponents of capitalism, intervene in the debate around cash? Nobody with a progressive perspective would want to preserve or even defend the widely-despised cash. Yet the fact is, compared to all other payment systems, cash is actually „coined liberty" (Dostoevsky). This is especially true for political activists, whose anonymity is a basic precondition for their political engagement!

As computer supported alternatives to cash, using the previously suggested crypto-funds such as Bitcoin in your everyday purchases require the use of a mobile computer with internet access, so a smartphone. However with smartphones there is no level of anonymity.

Conclusion: An unrestricted and anonymous alternative to cash is (at the time being) not in sight. Cash can be used to pay for things without the help of technical devices and (still) without fees. Aside from video recordings at the cashier, it doesn‘t leave any automatically saved traces of data behind.

More importantly: it prevents the permanent exclusion of all those that don‘t have any account at all, because they‘re not credit-worthy, because their life score is too low, because they are a refugee, because they are without work and a home. Bitcoins are an important, anonymous alternative to cash, yet only for those with computer proficiency– they‘re not useful for everyday activities (like buying peanuts at the liquor store) and is only for those that have access to a computer.

For these reasons, it‘s necessary to make an offensive demand for the retention of cash in all areas of our everyday life and unleash political pressure on the enemies of cash.

We haven't lost, we just haven't won yet

Emancipatory Beacon In An Increasingly Sinister Digitalized World

In response to the aforementioned scenarios, in this article we would like to point out ways to oppose the digital grasp and total surveillance. Not all battles targeting the internet and the "digital revolution" have been lost. On the contrary: we live in historical times in which great changes are descending on us in ever shorter intervals. These "developments" will determine our lives and behaviors for the coming decades. But they are not unstoppable and can be rejected. Nevertheless once integrated into our daily lives, it will be more difficult to reject the dynamics involved.

No question, states and companies have launched great attacks on privacy, anonymity, decentralization and self-determination. As their propaganda suggests, some of their success seems to be unavoidable and irreversible. But up till now, life without Google, Apple and Facebook is still conceivable, even if many people don't see it as something worth striving for.

Opposition against further control and influence is growing. A number of planned mechanisms of control have not been introduced due to a lack of acceptance. In a couple of years this development could progress so much that living without these technologies would mean being ostracized from society. If resistance doesn't pick up fast, a return to a life without these mechanisms of control will become as good as impossible.

In the following, we would like to name different possibilities of resistance with different aims and give examples of cases where they've already been used. It's necessary to keep in mind that resistance can become possible and effective. The technical possibilities that present themselves will unfortunately only be named in this text. That shouldn't prevent anybody from reading further into them.

ON ALL LEVELS

Resistance against digital control on different levels is possible and necessary. It can be successful if the practices on these different levels support and complement each other to impact society. Encrypting communication and using and developing alternative platforms as well as hacking surveillance firms belong to the *technical level*. The *political level* includes identifying and scandalizing surveillance firms, fighting against data-storing or discussing free internet. On the *legal level*, attacks on current developments in Facebook's private data storage are part of the strategy. Counter attacks are needed on all levels.

FROM INDIVIDUAL PRACTICE TO SOCIAL CHANGE

A first and easy step is the personal refusal of anything that imposes on one's self-determination. The next step is to organize this practice collectively and enable others to do the same. The goal is to create a widespread experience that can be shared by a significant mass of people over the time so that the practice becomes increasingly accepted in society. This has either already changed social processes or will indirectly lead to such changes. Other methods of resistance focus directly on the transformation of society. An example is raising awareness of particular problems. Publishing certain information helps, as do campaigns or exemplary court cases.

DEFENSE: ABOUT DIGITAL SELF-DEFENSE

Personal self-defense is the starting-point for defense against the increasing collection of data and the complete digital grasp. That means preventing one's data from being accessed by private organizations, internet service providers, mobile services, mail providers, internet advertising agencies, employers etc. This also includes civil services and public authorities such as intelligence agencies, social authorities, investigative authorities, financial authorities, customs, etc.

Using "strong encryption" for saving data on hard drives, USB sticks etc. as well as for transferring data helps. In the first case we recommend data encryption *DM-Crypt* for the Linux operation system. In the second case an effective encryption of mails by *PGP* or *GPG* is possible. Chat and other so-called instant messenger services can be encrypted by *OTR* (Off The Record). Another possibility is the ZRTP protocol (PGPFone) with which secure (according to current standards) calls can be made via VOIP .

Any other communication in the internet should at least be encrypted by SSL (HTTPS). This will not keep public authorities in particular from spying on transferred data. Nevertheless it offers at least minimal security against most private economic

agents. Another course of action to protect one's own private sphere is to produce a minimal amount of personal data. The basic requirement is to stay anonymous on the internet. Using the *TOR* (The Onion Router) browser enables precisely this. Even if in the aforementioned forms of communication data is encrypted (GPG, OTR), it still can still be seen who is communicating with who. In a lot of cases, that is more interesting and relevant than the content of the conversation itself. Anonymously created mails (via *Tor*) and chat accounts help protect against an investigation of who is communicating with who.

For instructions on the use of the technologies mentioned above we would refer our readers to our blog *https://capulcu.blackblogs.org*. There you will find the current edition of our first issue *"Tails – The amnesic incognito live system"*.

Give data sparingly – Generally speaking, it is necessary to produce and convey as little data about oneself as possible. This includes refraining from services such as Facebook, Google, Twitter, etc. which collect data on a mass scale, saves and evaluates it. There is no secure way of using these services. The same applies to smart phones with active WLAN, bluetooth and GPS. We would advise against using them.

It's necessary to develop a new way of thinking about the data one is prepared to give away. Once data is obtained, there is a high probability it will never be erased. Sharing data should not only be done sparingly, but also strategically: combining all the different activities, interests, passions, shopping activities and communication into an integral digital "identity" is the foundation of spying tools' power. To fight this, it helps to segregate our internet identities according to different activities, so that we have separate internet identities.

To buy a book, you don't need to provide a data farm at the other end of the world with your address, banking data and a list of all the products you've looked at before. One can simply go to the local bookstore next door and pay for the book in cash.

Since Snowden's revelations it is common knowledge that different producers of proprietary soft- and hardware build loopholes for surveillance into their products. This happens for reasons of personal interest as well pressure from public authorities such as the FBI or NSA. The use of open source soft- and hardware enables one to test out whether or not additional functions have been implemented to enable surveillance. An example of such a test was the crowd-funded investigation of the encryption software TrueScript. The software's source code was tested for intentional or unintentional loopholes (source code audit) or mistakes.

It is not enough to use Tor and TAILS to ensure our personal encryption. A collective approach needs to evolve from taking these steps towards self-determination and self empowerment.

One step would be to spread these forms of resistance and provide access to the tools and the knowledge of how to use them. That means that users should get together to solve problems together.

Another step would be to organize the development of those techniques. Joining the *Tor* project is an example (*https://www.torproject.org/*) or the Tails operating system (*https://tails.boum.org*) or developing simple methods of encryption (*https://leap.se and https://bitmask.net/*). Additional collectively developed software tackles the problem of how to use Google without being identified personally (http://www.googlesharing.net). The Guardian project provides tools that enable safer communication with Smartphones (*https://guardianproject.info*).

Any transaction with credit cards, cash cards, or pay cards is recorded forever. That is a reason to defend cash as a medium of exchange that eludes control. Bitcoin is an alternative medium of exchange on the internet that helps to mask and obstruct the traceability of monetary transactions. The established open source software in the Bitcoin network enables transfers *under pseudonyms* without regulating authorities. This is another advantage of Bitcoin accounts: the money that goes into them cannot be frozen by the government. Furthermore it can be saved on a stick. A detailed description of the function and the technical realization of actually anonymous money transfer cannot be given here.

...SPEAKING OF SOCIAL REJECTION

Digital self-defense and data frugality are insufficient to forgo the process of centralization, overall grasp, and total control in the long run. It is necessary that the technological attack on the entirety of society be countered by an attack from the entirety of society itself. Only then it will be feasible to build up means of self-determined communication. The goal is to establish resistance as a broad social practice.

An example of widespread social resistance are the protests against data-storing in Germany, against SOPA (Stop On-line Piracy Act) and against ACTA (Anti Counterfeiting Trade Agreement). Mass demonstrations, legal resistance and lobby work complemented each other well in this case.

In Germany 34.00 people joined a mass lawsuit against data-storing initiated by AK between 2006 and 2010. The goal of the lawsuit then was to prevent storing unsuspicious personal telecommunication-related data. The lawsuit ended successfully in 2010 with the verdict of the Federal Constitutional Court that the storage of data

in the suggested form was unconstitutional. Hence for the time being, the storage of personally related data was legally prevented in Germany. This legal success cannot be separated from the political and technical alternatives of the campaign against data saving. But the law was prevented on the legal level in the first place. Successes like are short-lived, as became evident in the German government's effort to enforce data-storing in the wake of the attacks in Paris in January 2015. Another initiative that is taking small legal steps to maintain data-sovereignty in an almost hopelessly lost territory is the initiative Europe vs. Facebook (*http://europe-v-facebook.org*). Its goal is to make it so that Facebook acts according to legal requirements. To do so, 10,000 users are going to the European Court of Justice.

CREATING ALTERNATIVES

The second strand of the more technological approach is using and creating alternatives. Merely rejecting certain technologies and methods won't be enough to act progressively on the long run. Developing open source hard- and software is crucial for emancipatory communication because it provides a basis for trusting in the infrastructure we use. That sounds very ambitious and is simply not possibly for most of us.

In practical terms, creating alternatives means countering dominant centralized technologies with our own techniques that offer more self-determination and anonymity. In doing so, decentrality is the central concept. Centrality inevitably brings about power structures. Alternatives are decentral autonomous systems that are ideally administered and developed by the user (or at least by members of a community). Decentralizing services, infrastructure and technologies has the effect of bringing them closer to the users, thereby making centralized control more difficult. Both counteract the trend of increased controllability and surveillance and can lead to more manageable, self-determined structures. What is important in this context is regaining control over one's own data.

Concrete practices could include hosting your own data on a self-run server. For example the arkos Project (*https://arkos.io/*) offers a simple possibility. A good overview of technological alternatives that try to escape increasing surveillance can be found on *https://prism-break.org*.

Setting up, administrating and providing internet infrastructure for individuals, groups and movements is the self-defined mission of many tech collectives in different countries such as: *riseup.net, tachanka.org* in the USA; *nadir.org, systemli.org, so36.net* in Germany; *inventati, autistici, noblogs, paranoici* in Italy; *boum.org* in France and *immerda.ch* in Switzerland. With collectively run servers they provide email services, webhosting, vpn, chats, Domain Name Services an many more. Their work offers an important basis for anonymous (as much as possible) com-

munication on the internet. Their experiences will play an increasingly important role in the future.

The backbone of the internet is administrated and controlled by a small number of big companies and states. For example a large part of internet connections made in Germany are forwarded over DECIX in Frankfurt (Main). This is a so-called *Peering-Point*, where German and international internet providers exchange data. Likewise data between countries and continents is exchanged by a very small number of submarine communications cables. In doing so, states and companies often have absolute control of these connections. Hence whole countries, single network areas or single users can be controlled, logged or blocked by the push of a button. Even in our own cities a small number of providers can shut down the internet if revolts or riots break out. In these cases, having a decentralized network infrastructure reduces its ability to be controlled and attacked.

The German project Freifunk (*https://freifunk.net/*), which creates an independent internet network based on open-access WLAN-routers, is a good example of said decentralization. Especially in France similar projects have established a well and truly alternative network. In other countries similar projects exist as well, for example in Greece (*http://www.awmn.net/*) and Spain (*http://guifi.net/*). The DIY ISP initiative (*https://www.diyisp.org*) was founded in 2013 in order to facilitate the transfer of knowledge between do-it-yourself (diy) internet service providers and to help new initiatives get started (*https://www.diyisp.org*).

Indymedia and Lorea as social groupware- For an introduction to alternative communication platforms it's worth having a closer look at a project everyone has used in one way or another: Indymedia. What started at the turn of the millennium as a source offering independent and self-determined media coverage for the anti-globalization movement has been used as an important news platform up to today. Nowadays the concept of a single platform may seem to be an obsolete way of spreading information with the many doors opened by blogs, Twitter and other so-called social media platforms. Nevertheless, with its many local IMCs (Independent Media Centers) and by developing its own software (MIR) run on its own infrastructure, Indymedia represents a collective approach to combining emancipatory processes with the use of technology.

Another example of combining technical tools with social movements in a collective process is the Spanish network Lorea (*lorea.org*). Lorea and its software is simply a social media platform. It was introduced during the Spanish M31 protests, the movement of the squares and demonstrations when participants expressed a desire to build digital networks, to get organized without using existing platforms, especially Facebook. What was advantageous for Lorea's development is that Facebook is far less accepted by Spanish activists (compared to Germany) and that

they are much more willing to look for alternatives. This, combined with the fact that there were people willing to offer and help develop this alternative right from the beginning of the protests resulted in Lorea being actively used by a very large community even today.

But Lorea is a Spanish network and there's no German equivalent. This is mostly due to technical reasons based on its fundamental architecture. Lorea adopts a centralized approach. The alternative to this is a so-called federal approach. It is up to internet activists to determine if an emancipatory practice can evolve from a tool. With this approach, practically everyone who has the technical know-how could run their own servers with independent databases and content. However these servers would still be available and connected within the network. Diaspora (diaspora.org), a project that's often said to be an alternative to Facebook, uses this federal approach. Without going any further into detail, we think that Diaspora has failed to be an alternative to Facebook.

Trapped in Facebook's and Twitter's social network - To the question how activists can spread content and mobilization on the internet, we unfortunately can't get around Facebook (a critique on Facebook can be found here: *https://www.nadir.org/txt/We_need_to_talk_about_Facebook.html*). As mentioned above, we are confronted with the problem that no similar tool is available. Therefore we have to return to traditional solutions. One way is an own website either with its own domain address or as a subpage of an already-existing one. This website should preferably be hosted by a leftist tech collective. However one needs to have skills in web programming. It is easier to use already existing Blog systems. Noblogs.org and blackblogs.org are based on the widespread Blog system WordPress and they offer a quick and easy way to create a website.

Twitter can be used comparatively anonymously and is widely read. It is chosen almost by default and is very popular for mobilizations and live coverage of actions. Up till now Twitter hardly ever intervenes– yet the dependence on their service still remains. But it is hard for independent alternatives to exist on the so-called social web. Most of the time there are no communities who should be reached out to. Therefore, independent alternatives such as *friendica.com* or the microblogging service *indy.im* are being ignored. No one bothers to support them by creating a profile, which would make them more attractive for others.

Wikis and Etherpads - Public and private wikis are a tool that can be used for considerably large organizing processes. Lots of projects use wikis to have discussions, to release documentations or as a simple website. Yet to take full advantage of wikis one needs to have a bit more technical know-how. Especially if you want to set up a wiki on a server. With a little practice, wikis are easy to use. A wiki that is easy to

use is crabgrass on we.riseup.net. However, this project is frozen at the present level and will not be developed any further. But it can still be used. So-called Etherpads (*https://pad.systemli.org* or *https://pad.riseup.net*) can be used for writing and editing texts collectively and for organizing on a smaller scale.

HACKING AND SABOTAGE – ONLINE AND OFFLINE

Aside from creating our own infrastructure and advocating the necessity of digital self-defense, the third practical approach described in this text is actively blockading or sabotaging. This means (digital) attacks against structures of surveillance, control and the maintaining of capitalist power.

One praxis is **leaking** [das Leaken], i. e. publishing classified information. This can make information available to the public as well as create scandals. In some cases the information provided clears the way for further attacks. A current and prominent example for leaking is the hack of FinFisher, a company specializing in surveillance. In June 2014, an anonymous hacker hacked one of the company's web-servers an published 40 GB of data. This data contains the company's correspondence with its clients, the customers' information files, price lists and manuals which are otherwise not available to the public. Among others the source code of FinSpy Mobile and FinFly Web (software used to spy on smartphones) was published. That is a substantial problem for the company as companies providing antivirus software now are able to detect and neutralize this malware. In the communique *"Don't wait for the next whistleblower"* the hacker gives detailed information on their motivation, method and calls for further actions against surveillance companies.

Another fun thing to do is sabotage those who are responsible for and benefit from surveillance. In doing so, the availability of services or infrastructures are blocked. Alongside the cutting of wires, there are plenty of measures that can be taken to shut down servers, routers or similar network infrastructures either temporarily or for longer periods of time. If a web-server receives huge amounts of requests this may cause the server to be entirely unavailable. This can do lots of damage to the attacked provider. For example, in 2011 VISA was attacked by Anonymous in this way because it was one of the main protagonists responsible for freezing Wikileaks bank accounts. For a long while VISA's servers were only sporadically available, which lead to a significant amount of financial damage as well as tarnishing their public image.

IT systems are being attacked regularly to get information and to make it available to the public. In August 2008 antifascists hacked the Blood and Honor network and published the addresses and photos of its members. In July 2011 the so-called PATRAS system was hacked by „No-Name-Crew". The system is run by the

German Bundeskriminalamt (BKA, Federal Criminal Police Office), Landeskriminalamt (LKA, State Criminal Police Office) and Zoll (Federal Customs Service) and uses GPS tracking devices to monitor suspects and goods.

Just as in the "offline-world", there are demonstrations in cyberspace. The aim is to call on a certain homepage repeatedly from many computers during a fixed period of time in order to block the server the homepage is located on. If this is successful, the homepage will either be unavailable or slowed down considerably. The first online demonstration took place in December 1995 and was directed against the French government in response to its nuclear weapons test at the Mururoa atoll in the Pacific Ocean. Since the internet was not very popular then, the demonstration had only limited success. In June 2001 a demonstration against Lufthansa elicited huge media response. The action was taken as a part of the antiracist „Deportation-Class" campaign organized by German activists, which criticized airlines for taking part in state-run deportations. The company's website was hardly available at all during the two hour blockade.

In the end of November 1985 anonymous activists vented their rage on the planned privatization of Japan's state-run railroad company. Early in the morning they simultaneously cut altogether 30 computer network cables at different places. This had devastating consequences: In Tokyo, Osaka and five other major cities railroad traffic broke down with one single stroke. Ten million commuters arrived to work very late or not at all . As a result, banks and businesses were short of staff, schools stayed closed and at the stock exchange in Tokyo, there were only a few brokers. The government said it was „by far the most damage done by a guerrilla action in many years". Similar actions were taken in Germany: in February and July 1996 fiber optic cables around the Frankfurt airport were cut to point out the role it played within the „imperialist world order", to demand open borders and to stop deportations. These and other actions have proved the vulnerability of performance-based data networks ever since.

Even a company as big as Google appears to be extremely sensitive when it comes to social resistance. When shuttle busses were stopped and attacked several time in San Francisco in 2013, Google was very concerned. With these actions, people protested against enormous rent increases in the commuting area of the air-conditioned luxury busses that drive Google employees to the company's headquarters. After the initial deployment of Google Glass in the USA, many arguments or fights broke out because some people were worried about being secretly recorded or directly „scanned". Lots of bars and clubs took part in the campaign against Google „*Glassholes*" and threw out people wearing Google Glasses to protect their customers. In 2015 Google stopped selling the first version of the smart glasses, citing a lack of acceptance. However behind the scenes it is still developing a follow-up model.

Big Data

>Esc
>Del
>Shutdown
>Reboot

Life is no Algorithm
Collective Perspectives
against the technological Attack

Cologne | 30.09.- 02.10.2016

bigdata.blackblogs.org

keep the future

Our refusal
to take part in the
permanent digital transmission,
our struggle to defend ourselves
from the digital attack are insufficient
measures in the attempt to remove
ourselves long-term and completely

from ~~surveillance~~
and heternonomy

A counter-attack on
the praxis and ideology of
total acquisition is absolutely
necessary.

unwritten

capulcu productions 2015