Digital Tailspin

Ten Rules for the Internet After Snowden

MICHAEL SEEMANN

Network Notebooks 09

Digital Tailspin

Ten Rules for the Internet After Snowden

Network Notebooks 09

NETWORK NOTEBOOK SERIES

The Network Notebooks series presents new media research commissioned by the INC.

PREVIOUSLY PUBLISHED NETWORK NOTEBOOKS:

Network Notebook 08

Brooke Wendt, The Allure of the Selfie: Instagram and the New Self Portrait, 2014.

Network Notebook 07

Henry Warwick, Radical Tactics of the Offline Library, 2014.

Network Notebook 06

Andreas Treske, The Inner Life of Video Spheres: Theory for the YouTube Generation, 2013.

Network Notebook 05

Eric Kluitenberg, Legacies of Tactical Media, 2011.

Network Notebook 04

Rosa Menkman, The Glitch Momentum, 2011.

Network Notebook 03

Dymtri Kleiner, The Telekommunist Manifesto, 2010.

Network Notebook 02

Rob van Kranenburg, The Internet of Things, 2008.

Network Notebook 01

Rosalind Gill, Technobohemians of the New Cybertariat, 2007.

CONTENTS

ACKNOWLEDGEMENTS — 5

INTRODUCTION — 7

RULE 0: EVERYTHING STAYS DIFFERENT — 11

RULE 1: YOU CAN'T FIGHT *KONTROLLVERLUST* — 15

RULE 2: SURVEILLANCE IS PART OF THE GAME — 18

RULE 3: KNOWING IS ASKING THE RIGHT QUESTIONS — 25

RULE 4: ORGANIZATION AND CONFLICT FOR FREE — 30

RULE 5: YOU ARE THE FREEDOM OF THE OTHER — 35

RULE 6: PLATFORM CONTROL IS POWER — 38

RULE 7: THE STATE IS PART OF THE PROBLEM, NOT OF THE SOLUTION — 44

RULE 8: DATA CONTROL CREATES HEGEMONY — 49

RULE 9: AND THE FINAL BOSS IS... US! — 56

REFERENCES — 61

COLOPHON

Network Notebook #09
Michael Seemann, Digital Tailspin: Ten Rules for the Internet After Snowden

This text is a translated and updated excerpt of *Das Neue Spiel: Strategien für die Welt nach dem digitalen Kontrollverlust*, Freiburg: Orange Press, 2014. Translated from the German by Anwen Roberts

Network Notebooks editors: Geert Lovink and Miriam Rasch
Design: Medamo, Rotterdam http://www.medamo.nl
EPUB development: André Castro
Copy-editing: Margarita Osipian
Printer: Printvisie
Publisher: Institute of Network Cultures, Amsterdam
Supported by: Amsterdam University of Applied Sciences (Hogeschool van Amsterdam), Amsterdam Creative Industries Publishing, Stichting Democratie en Media

If you want to order copies please contact:
Institute of Network Cultures, Hogeschool van Amsterdam
http://www.networkcultures.org
books@networkcultures.org
t: +31 (0)20 59 51 865

EPUB and PDF editions of this publication are freely downloadable from:
http://www.networkcultures.org/publications

Amsterdam, March 2015
ISBN 978-90-822345-8-9 (print)
ISBN 978-90-822345-9-6 (EPUB)

Acknowledgements

Many of the ideas presented here were developed over a number of years and in constant exchange with others on the net. More so, the entire project rests on the shoulders of many, as it was realized with a crowdfunding campaign. The writing of this book would have never been possible without the help of a number of people.

I'd like to thank Geert Lovink, Miriam Rasch, and the Institute of Network Cultures in Amsterdam, for allowing me to publish an international version of my thoughts.

Many thanks to my translator, Anwen Roberts, for rendering my work into concise English and to my editor Valie Djordjevic, who has repeatedly nudged me back onto the track of legibility. It has been a great collaboration.

A big thank you to the 'beta readers' who endured – and improved – my half-baked notes and outlines, especially Leonhard Dobusch, Caspar Clemens Mierau, and Jürgen Geuter.

Sincere thanks to Mark Wirblich and Maria Thaens, who afforded me shelter in their agency Bytes Brigade; the most beautiful office in Neukölln. Special thanks to Jörg Leupold, who in the past six months of madness spent those rare moments of spare time with me, and helped me to regenerate.

My gratitude to everyone who supported me in setting up the crowdfunding campaign and helped with the campaign video. I would particularly like to thank Mate Steinforth (camera), Gerlinde Schrön (editing), and Mark Wirblich for the original cover design.

And last but not least, my heartfelt thanks to all the crowdfunders who donated their money and trust, and without whom this text would not have been possible at all.

Introduction

> *Yet as we unleash living forces into our created machines, we lose control of them.*
> Kevin Kelly

In 2008, although I had been an active blogger for three years, I had only quite recently joined the online messaging service Twitter. It was a time of discovery and experimentation with new forms of social communication on the internet. In the German-speaking world in particular, the number of people prepared to discuss personal matters online and share their opinions on a larger scale was still very low. To me, the possibilities were inspiring and at the same time rather scary.

I was aware that data protection was important, and I was seriously concerned about privacy online. The reasons were twofold. For one, I was making a living from web programming at the time, so I had to deal with databases and data models on a daily basis. This had given me some idea of how powerful they were. I was becoming more and more involved with what is now probably best described as the German internet movement: a loose network of hackers, bloggers, and activists, who saw the internet primarily as a political space, a zone of freedom that was worth preserving. In the tech scene, there was never any doubt that privacy was a valuable good that needed extra protection.

At that time I wrote an article about the perils of Twitter.[01] Two incidents had inspired me. One was that Twitter user Matthias Bauer (@moeffju) would regularly tweet something like 'So that's that. #Feierabend' as soon as he finished work. (*Feierabend* being the German word for closing time, as well as the evening off that follows.) Words tagged with the hash symbol in this way are more easily found in a search on Twitter. A search query for the term 'Feierabend' would spit out all the tweets mentioning this hashtag – and most of them were from @moeffju.

The other incident was an article written by Twitter user Markus Angermeier (@kosmar) in which he explained, among other things, how he sent people birthday wishes on Twitter. He would use the hashtag #hpybdy in his congratulatory tweet and in that way create a birthday calendar of his own along the way.

In my article, I tried to envision the impacts of this kind of behavior. With sufficiently powerful data analytics, it would have been easy to create a profile of @moeffju's working hours. Future clients or employers could take one look at his schedule and draw conclusions about his motivation or diligence. And @kosmar's birthday ritual amounted to compiling a complimentary list of active Twitter users' birthdays, even though they might never have made that date public themselves. Because the date of birth is such an important data point of identification, @kosmar's birthday logs were a danger to all those people who wanted to travel the web anonymously.

Ordinary social practices that seem innocent at first glance may have unexpected consequences as soon as they are made searchable and connectable. 'I do not yet know what all of this means for me and my tweeting,' was how I ended the article at the time. Today, I know this was the starting point of a broader contemplation of the matter, which has, with some diversions, led up to *Digital Tailspin: Ten Rules for the Internet After Snowden.*

---

01 | Michael Seemann, 'Profiling mit Twitter, oder was ist ein Captcha?', http://mspr0.de/?p=568.

First, I pursued my thoughts about *Kontrollverlust*, the loss of control in the digital world, only casually.[02] But when Frank Schirrmacher, the late editor of German daily *Frankfurter Allgemeine Zeitung* (FAZ), asked me if I wanted to write a blog for the FAZ website in early 2010, I knew this would be my topic. My blog was aptly named 'CTRL-Verlust'. Unfortunately, the collaboration ended after about six months due to a conflict of opinions with the editors, but I continued the blog by myself at *ctrl-verlust.net*.[03]

THE BOOK

Over the past four years I had occasionally thought about turning my increasingly extensive body of reflections on the digital information tailspin into a book. But somehow, the final incentive was missing. What tipped the scale were Edward Snowden's revelations in 2013. The monstrosity of this gigantic project – nothing less than the observation of the entire planet – made me realize just how small I had been thinking until then. So far, I had regarded *Kontrollverlust* as an everyday phenomenon that was still quite rare, but might impact one person or another. That it had long become the totalitarian reality of every single person on the internet surprised me.

I'm certainly not the first one to regard this framework as a 'game changer': a shift in circumstances with the power to modify the coordinates of the world and radically change the rules of the game. But I may be the first one trying to formalize these new rules. The German title of my book, *Das Neue Spiel: Strategien für die Welt nach dem digitalen Kontrollverlust*, translates to *The New Game: Strategies for the World After the Digital Tailspin*. The *Ten Rules* you have in hand are a modified version of the second half of the book.

THE CAMPAIGN

Writing a book about *Kontrollverlust* is one thing. It is another to write it in such a manner that the concept matches its contents. If I assume that data is uncontrollable, I can't just go to some publishing house and publish a book under the usual conditions of copyright. A different solution had to be found. I devised a crowdfunding campaign that allowed me to collect money before publication; enabling me to write the book without any advance payment from a publisher.[04]

The campaign cost a lot of time and effort, but it was worth it. Instead of the 8,000 euros I had set as a target, I collected a total of more than 20,000 euros, making the campaign the third most successful crowdfunded German-language book project at the time. The edition at hand is borne of this success: the translation of *Ten Rules* was a so-called 'stretched goal', one to be realized in case the 20,000 euro mark was reached.

---

02 | We chose to keep the German word *Kontrollverlust* in the English text, not least because of the difficulties in finding an appropriate English equivalent. The German *Kontrolle* has different connotations, with a stronger focus on governance, or supervision, than on the steering or driving mechanisms that the English term 'control' emphasizes. *Kontrollverlust* occurs whenever the behavior of information changes in such a way that it systematically fails to match prevailing expectations.

03 | Michael Seemann, 'CTRL-Verlust', http://www.ctrl-verlust.net/.

04 | My Startnext crowdfunding campaign can be found at https://www.startnext.de/ctrlverlust/.

THE LICENSE

As part of the campaign, I designed a license for the book and the *Ten Rules* in collaboration with iRights.info.[05] The license is called the WTFPDL, a derivative of the WTFPL, the 'Do What The Fuck You Want To Public License'.[06] My extension basically consisted of inserting the D, for 'Digital'. While the original license model literally permits any conceivable use, my extended version grants this right in the digital domain only. In the physical world, for printed books for example, the digital license is not valid, and normal copyright applies instead.

In this respect, the WTFPDL license demarcates the fault line between the Old and the New Game. In the Old Game – a world of walls, distances, masses and bodies – the old rules apply: copyright laws. In the New Game – a world in which data is freely copied and recombined – the loss of control comes into full force, unrestrained.

The book, the crowdfunding campaign, the license, as well as the English version of the *Ten Rules*, are all part of the same work. All these elements respond to the challenges of the digital tailspin in their own way, and are intended as guidance to, or examples of, how the future might look in the New Game.

So much for my history with *Kontrollverlust* – from this point on, let's follow the rest of the story together.

KONTROLLVERLUST: LOSING CONTROL

Current debates about copyright, privacy, failed corporate communications, state secrets, whistleblowing, or spontaneous network phenomena like flash mobs and hashtag revolutions, are all manifestations of one and the same issue: the loss of control over data on the internet.

Kontrollverlust produces an incredible dynamic, making it increasingly difficult to control who is producing, compiling, copying, or evaluating which information. The loss of control takes place on three levels, which I call *drivers*, because they are the motors powering the digital tailspin that awaits us.

1. Every last corner of the world is being equipped with sensors. Surveillance cameras, mobile phones, sensors in vehicles, smart meters, and the upcoming 'Internet of Things' – tiny computers are sitting in all these objects, datafying the world around us. We can no longer control which information is recorded about us and where.

2. A computer will make copies of all the data it operates with, and so the internet is basically a huge assemblage of copying machines. In the digital world, practically everything we come into contact with is a copy. This huge copying apparatus is growing more powerful every year, and will keep on replicating more and more data everywhere. We can no longer control where our data travels.

---

05 | iRights (Digital Copyright Information Platform), http://irights.info/.

06 | For the WTFPL, see: http://www.wtfpl.net.

3. Some say that these huge quantities of data spinning around have become far too vast for anyone to evaluate any more. That is not true. Thanks to Big Data and machine learning algorithms, even the most mundane data can be turned into useful information. In this way, conclusions can be drawn from data that we never would have guessed it contained. We can no longer anticipate how our data is interpreted.

In other words, data we never knew existed will find channels that were not intended and reveal information that we would never have thought of on our own. And this is substantially changing the world.

My theses are controversial within the German digital community, not least because they unveil the irretrievable end of privacy and are thus threatening one of the main pillars of a shared canon of values. But I haven't been entirely alone with this discourse: Christian Heller's concrete ideas pertaining to a post-privacy world,[07] as well as the formation of the 'privacy-critical alliance' Spackeria,[08] have in recent years repeatedly led to heated debates within the German net scene.

STRATEGIES

Technology neither determines social structures, nor does it govern our actions. It defines a room for maneuvering that can be shaped politically. Technology makes certain strategies more effective, and sentences others to failure in the long run.

What constitutes a good strategy is not the same for all players in the game. Our standpoint is one of an emancipatory global civil society, which we are part of ourselves. From this position, we can assess the situation and promote strategies that will enhance the freedom of civil society while, at the same time, protecting the disadvantaged. Rather than giving instructions, I want to examine why some strategies are more appropriate in the New Game than others.

07 | Christian Heller, *Post-Privacy: Prima leben ohne Privatsphäre* (*Post-Privacy: Living just Fine Without Privacy*), Munich: C.H. Beck Verlag, 2011.

08 | 'Datenschutz-Kritische Spackeria', http://spackeria.org/.

Rule 0:
Everything Stays Different

Proposition: In the New Game, many timeworn certainties have been rendered invalid. In order for us to understand and profit from new opportunities, and identify new threats, we need to actively unlearn the old and engage with the new wholeheartedly.

First things first. The rule preceding the rule. Programmers commonly start counting at zero, instead of at one. Zero is the blank slate; the empty set that makes sure we do not yet know where we are going. Because normally we will already be somewhere, we will have preconceptions, and that is precisely the problem. Therefore, Rule Zero. Before we begin we first need to take a step backwards, away from the first step, away from our misconceptions, and go back to zero.

If the problem at hand were only the uncertainty of the future, it wouldn't be half as bad. That is something we can handle, something we don't need a rule before the rule for. The problem is, of course, that we are human. We believe that we can make assumptions about the future based on our experiences in the present and the past. We tell each other stories, extrapolating their meaning into the future, and use statistical analysis to calculate the probability of events. We anticipate trends and develop scenarios, perform risk analysis and determine the likelihood of disasters. We are perpetually consulting the past in order to predict the future. What could possibly go wrong?

Researcher of randomness and former financial analyst Nassim Nicholas Taleb alerted the world to the major role of unpredictability in his 2007 book, *The Black Swan*.[09] In his book Taleb demonstrates how rare and improbable events, typically not covered in any plan or scenario, have repeatedly become major turning points in history, often with disastrous effects. To paraphrase Donald Rumsfeld, former US Secretary of Defense: in addition to the knowns and the unknowns (which we know that we know nothing about), there are also the 'unknown unknowns' – those unexpected items that we don't even know we should know about. This is what the eponymous 'black swan' refers to: before the European exploration of Australia in the 17th century, no one in Europe even knew that black swans existed, since local everyday observation suggested that 'white' was one of swans' defining properties. So when black swans were finally documented it was clearly a turning point in terms of swan research, moreover, an event calling the entire concept of swans into question.

Taleb calls this specific arrogance regarding the future the 'Platonic fallacy'. We are prone to confuse the theory, the model, or the abstract idea with the thing itself, provoking a false sense of security. We believe we have some understanding of the outside world, but in fact, our supposed wisdom distorts our worldview. Another distortion that Taleb explores is the 'narrative fallacy', which allows us to rationalize random events by incorporating unrelated facts into our stories in retrospect.

What is new always happens unexpectedly. We do not notice what is going on, mainly because we have no idea what we are looking for. Change comes to the world largely un-

09 | Nassim Nicholas Taleb, *The Black Swan: The Impact of the Highly Improbable*. New York: Random House, 2007.

detected, will only gradually gain traction, and is, by definition, beyond our control. So let us try to liberate ourselves from our prejudice against the new, and forget what we once thought was true. Let us scrutinize everything, take nothing for granted, and distrust those who claim to have 'known all along'. In the New Game, the rules have changed so fundamentally that many aspects need rethinking. In such situations a certain reluctance to get off the beaten track is quite natural. But what was good before may suddenly turn stale. What used to be a promise of freedom could be a new kind of prison today – or vice versa.

THE EMPIRE STRIKES BACK

'Institutions will seek to preserve the problem for which they are the solution,' Clay Shirky once said.[10] We live in a world today where the music industry is one of the greatest obstructers of music distribution. In its quest to suppress the online exchange of music (something that for all intents and purposes could be attainable for everyone at low or no costs), the music industry has tried to exploit any legal and promotional leverage it could find. The sector has a history of filing lawsuits that have ruined entire families, locking up videos on video platforms, and censoring search results and the internet at large. Currently, the greatest enemy of music on the web is the music industry itself.

The news media seem to be up in arms against the informed public now too. In Germany, corporate publishers and news outlets lobbied and lobbied until the (subsidized) public broadcasting system was finally forced to oblige: public broadcasters are now permitted to make their content available online only for a certain time. News items will usually disappear from the web after seven days. *Depublizieren* (un-publish) is the peculiar term coined specifically to refer to this practice of rendering published content, which is largely financed by the German public through license fees, inaccessible again. The news media even managed to lobby their way into federal legislation with the infamous *Leistungsschutzrecht*, an ancillary copyright law specific to German corporate publishers. With that, news media are basically trying to cash in on search engines via legislation, all the while profiting from the attention and publicity that their content gets through Google and others.[11] Fearing its own demise, the press has now become one of the worst enemies of the public.

We should start to purposefully distrust the old. The old ways will always consider themselves indispensable. The old will always try to prove that without it the decline of the West, or democracy, or the world in general, is nigh. It would be a mistake to listen to the ones losing out in this situation of upheaval. We must be wary of placing the individual cases of a privileged few above the common good. And we must avoid sacrificing the opportunities of digitalization to a past that, anyway, will never return.

---

10 | Liz Gannes, 'SXSW: Shirky's New Opportunities in Public Sharing', *Gigaom*, 14 March 2010, http://gigaom.com/2010/03/14/sxsw-shirkys-new-opportunities-in-public-sharing/.

11 | 'Leistungsschutzrecht (translation: ancillary copyright) is a bill in Germany. It would give press agencies the exclusive right to publish press releases for commercial purposes on the Internet and would require search engines such as Google to obtain licenses for using small text passages.' Wikipedia contributors, 'Leistungsschutzrecht', 4 March 2013, http://en.wikipedia.org/wiki/Leistungsschutzrecht, accessed 16 January 2015.

NEW THREATS

If you take such a dispassionate look at the disruption of the old, you are quickly accused of being a naive internet utopian, expediently choosing to see only the good parts. That is not the case. To recognize the new as being new, and to stop mourning the outmoded, does not necessarily imply that change should be celebrated uncritically. Quite the contrary. There are many new hazards brewing in the New Game. But alarmists, instead of observing the situation closely and articulating legitimate criticism, tend to obstruct our view of the real challenges. That is to say, the challenge at hand is not just the demise of the old. We do not need to worry about there being no more music or no more journalism.

It is evident that change not only yields new opportunities, but also brings new dangers – dangers that are not recognized as such precisely because of their novelty; they are black swans. We need an unclouded view to be able to recognize these threats, just as well as the opportunities. The struggle so far has not been between utopians and realists, but rather between realists and nostalgics. The New Game has already begun, it is already changing the world, change is already a reality. It is time to leave the mourners behind.

STRATEGIES

Developing strategies against your own biases means closing certain doors and opening others. It means leaving your accustomed standpoint behind and taking an unusual stance. Two strategies can help.

SINKING SHIPS

In his book *Digital Renaissance*, the literary scholar Martin Burckhardt suggested that when dealing with the digital shift, we should adhere to a lesson provided by Spanish conquistador Hernán Cortés. As soon as his expedition had arrived in South America he sank the ships they had come on, right in front of his crew. That would leave them with no hope of ever returning to the old world – and with a blank slate, providing the mental state for them to deal with the new continent.[12]

Figuratively speaking, we need to demolish all hope of returning to the Old Game. The New Game is clearly not paradise on earth, is not inherently better than the old, but it is exciting and full of opportunities. New worlds entail risks that differ from those dragons of old. By mentally detaching from our old world we can free our minds to those new opportunities and challenges, as well as risks, that await us in the New Game.

LOOKING BACK AT TODAY

One interesting way of liberating our understanding of the present from the adhesiveness of current experience was presented by German media theorist Stefan Heidenreich. He invites us to participate in a thought experiment:

> Imagine yourself in ten years, looking back at what is now the present. The year is 2020, and maybe you will remember this text you read or heard a decade ago,

12 | Martin Burckhardt, *Digitale Renaissance: Manifest für eine neue Welt*. Berlin: Metrolit, 2014.

> maybe not. Maybe you were traveling. Maybe there is a picture that a stranger took of you on the street.[13]

In the year 2020 face recognition algorithms will be ubiquitous, so we will easily be able to reconstruct random encounters we had on the street. We can determine who else has read the same text, because we will all have left our digital traces. We will know a lot more about the past – that is, about today – than we know about our past today. Then we look back even further:

> Looking further back into the past, into the years 2009, 2008 or 2007, you will find the light cone of data fading. You will find yourself on the verge of a zone of darkness you no longer have access to. You may vaguely remember some of the data points beyond this light cone. But recalling the unlit past will seem increasingly tedious, because you know nothing for certain and can't check the details in any of the archives. This means that we are already in the process of leaving this area of darkness now, in our current years.

In other words: our future selves will experience a similar feeling of gloom assessing our present as we might today when looking at the Middle Ages. And in much the same way as we can barely understand today how people used to live in a feudal system, our future selves will not understand why some of us were so strongly opposed to the light.

13 | Stefan Heidenreich, 'Datendichte und digitale Geschichte', *Docupedia – Zeitgeschichte*, 11 February 2010, http://docupedia.de/zg/Blog:%22Datendichte_und_digitale_Geschichte%22_-_Vortrag_von_Stefan_Heidenreich_zur_Projektpr%C3%A4sentation_am_11.02.2010_2010/03/05]. (Translation by the author.)

Rule 1:
You Can't Fight *Kontrollverlust*

Proposition: If your strategy requires you to control the flow of information, you don't have a strategy.

The Old Game was based on the simple fact that information did not flow freely. The dissemination of information was expensive and, therefore, a very conscious act. Articulating and collecting individual interests and demands, distributing and processing information within and outside of organizations – these were well-negotiated, well-structured, and culturally ingrained procedures for a good reason. Data protection, legal protection of minors, censorship issues, state secrets, copyright, trade secrets, public relations strategies, etc., are all still based on these old and rather stolid mechanics of information exchange. Alas, these strategies are increasingly denying us service.

In the New Game, knowledge is created much faster and spreads uncontrollably. We need to brace ourselves for a world in which we can ultimately never know who has access to which information. This puts into question all those institutions and social procedures that have, so far, relied on old forms of information control.

STRATEGIES

Nassim Nicholas Taleb's 2012 book *Antifragile* addressed again the question of dealing with 'black swans' – that is, completely unpredictable events.[14] If we can be sure of one thing, it's that we cannot possibly forecast a black swan. So instead of focusing on risk management, Taleb asserts that we should make sure our systems – our enterprises, economies, and societies, as well as our own lives – are not fragile by design.

Robust systems that can endure anomalies and disturbances will remain in the same state as before, even after disruptions. A system that is fragile, however, will deteriorate or collapse entirely when disrupted. Taleb's model to counter this is the 'antifragile system', which, in fact, gets stronger with every interference. Its mythological role model is the Hydra. For every head that is chopped off, the Hydra grows two more.

This pattern is easily applied to our current problem with *Kontrollverlust*. A lot of strategies that were founded on the control of data have become fragile. Some new development in peer-to-peer technology pops up, and entire business models, seemingly secure until then, start to disintegrate. We thought state power could be fenced in using the state's very own data protection rules, but we didn't have the intelligence apparatus on our radar screens, operating – and co-operating – between, and well beyond, legal and national boundaries. Politicians believed they could speed up procedures by keeping negotiations secret, but intelligence agencies used this information against them. New journalism projects like WikiLeaks blew the whistle, and today we have young people on the streets protesting the secret negotiations of treaties like ACTA and TTIP. Generally speaking, the digital tailspin is an issue of strategies turning fragile.

---

14 | Nassim Nicholas Taleb, *Antifragile: Things That Gain from Disorder,* New York: Random House, 2012.

DISTRUST FRAGILE ELEMENTS

First, we need to identify fragile elements, and become skeptical of promises they can no longer keep. Privacy has gone bankrupt. The idea that an official state body could ensure that data is protected from abuse has turned out to be naive. On the contrary, if there is anything to worry about, then it is precisely those national and supranational organizations (the intelligence services are, in their present form, an inextricable meshwork of over- and intergovernmental threads) that defy any law regardless. Data protection presents itself today as an exclusive state monopoly of access and assessment privileges. The state is allowed virtually anything, while civil society is regulated.

Along with data protection the concept of privacy settings, as publicized by social networks, has also outstayed its welcome. Even if I only share my photos with friends, I'm sharing them with the network (such as Facebook) and with the NSA. If I chat with a friend online, I'm chatting with a friend and GCHQ. When I send an unencrypted email, I'm sending it to the recipient and to the BND.

Likewise, the whole idea of limiting cultural goods and knowledge in order to make money is becoming more and more outdated. The times when this system was able to adequately compensate creators are long gone, and things will only get tighter in the future. To be honest, only very few people ever benefited from this system anyway. Those who still expect their works to circulate only in the designated channels will surely not succeed.

ROBUST LIVES, ENTERPRISES, SYSTEMS

Although we can hardly foresee what will happen to any given information, nor comfortably make plans *with* the information tailspin, we can make our lives, our business models, and our societies adapt in such a way that they are less fragile when it comes to *Kontrollverlust*.

If you are successful in any sense of the word, you are clearly more vulnerable to the impact of the information tailspin than if you had 'nothing to lose'. It starts with the fact that burglars have more ways to determine whether you are at home. A successful career might make you a target for smear campaigns. Gaining a reputation of any kind will make you more vulnerable to people who insult, harass, or even stalk you.

An ideal, antifragile business model isn't based on scarcity. Take crowdfunding: you can present a project or enterprise you are planning and have it pre-financed by the 'crowd', for instance, by selling copies of a book before it is published. This book is an example of that itself. Moreover, it is being released under a free license. File sharing won't hurt it, because shared copies have already been priced in. The money has already been made. File sharing is not able to take away funds collected in advance.

Societies that are intolerant of differences in lifestyle are also fragile in times of lost informational control. The struggles against homophobia, racism, and prejudice enhance the robustness of the individual in the information tailspin because there is less to lose if everything can be open. Those forced to keep their sexuality a secret find no freedom. Still, it is less a matter of information control than a challenge for the whole of society to ensure that this kind of secrecy is unnecessary.

OPENING UP TO ANTIFRAGILITY

Building robust systems as a defense against the information tailspin will not be enough. We also need elements that respond to this loss of control in a positive manner, elements that are the opposite of fragile: antifragile.

One example that Taleb mentions involves the loss of information control directly. He describes his own profession as being antifragile against rumors and negative reporting in particular. He points out that as an author he could trigger a scandal at any time, and instead of having to resign, as a politician or a manager might be forced to, it would only improve his success and, of course, his book sales.

Strategies that rely on openness, transparency, and networked structures are antifragile in the information tailspin – think of the Free Knowledge, Open Government, Open Data, or Open Source movements. Every single item of information in the network allows for additional connectivity, and for most kinds of information this connectivity is, in fact, desirable. Our personal needs, our ideas, our vocations, and mindsets… many aspects of our personalities give us good reason to network with others, and it can be worthwhile to actively surrender to *Kontrollverlust*.

As an individual, you can expose your works and actions to valuable criticism, thereby making advances in your field. This already applies to programmers, for instance. As a politician, you can generate more trust if you decide to disclose as many processes relating to your activities as possible. As a writer, you will reach a greater audience with your ideas. As an activist, you will be able to find like-minded comrades faster. Informational openness thus is an antifragile strategy in times of the digital tailspin.

Rule 2:
Surveillance Is Part of the Game

Proposition: Surveillance will notably increase in the New Game, and we will reluctantly learn to deal with it. Effective action against surveillance will mean mitigating its effects.

They were exciting times, the early 1980s. Highly political times too, in the Federal Republic of Germany. Major policy shifts, such as the controversial construction works at Frankfurt airport ('Startbahn West'), the stationing of intermediate-range missiles, and changes in nuclear policies, had spawned a variety of social movements in Germany that were becoming increasingly vocal in protesting what had, in their mind, become an increasingly repressive state. And then the population census came. Its opponents managed to mobilize fellow campaigners far beyond the range of usual suspects from the peace and environmental movements. By March 1983, there were more than 500 citizens' initiatives working on the topic, and public opinion was starting to swing.

The German Federal Constitutional Court had already halted the census project with an injunction order in April 1983, but it still took until December 15th of that year before the Court repealed the entire census law as being unconstitutional. In the course of this landmark decision, the Court also decreed a new fundamental right: the right to 'informational self-determination'. This was directly derived from Article 1 of the German Constitution ('Human Dignity'), and its associated fundamental human rights. Since that day, the right to decide on modalities of publication and usage of personal data has not only become the legal basis of German privacy laws, but also a deep-seated cultural cornerstone of Germany's self-conception.

Thirty years later, in September 2013, the Germans elected a new parliament. Again, these were exciting times, and again, it had something to do with data collection. Four months before, Edward Snowden had launched his first revelations about secret NSA and GCHQ espionage programs. The German public learned the hard way that literally no one could make claims to 'informational self-determination' any more. The whole world was wiretapped, all the time and all over the planet, and everyone was affected. But while the news media were falling over themselves reporting and clarifying, while internet activists could hardly stop hyperventilating, while the greatest privacy disaster imaginable was taking its course, the general public seemed to take little interest in the matter.

In Germany the conservative party CDU, which had responded to the scandal in the most graceless and sedate manner imaginable, actually ended up gaining votes in the general elections, while the other acting government party at the time, the liberal FDP, which had shown at least some interest in a fact-finding investigation, was voted out of the Bundestag. The opposition parties, trying to use the scandal as political leverage against the government, were not rewarded either. The German Pirate Party, whose core topics include privacy and surveillance issues, failed again to enter parliament, garnering only 2 percent of the votes.

So here's the bad news: neither state-aided, nor economic, nor private surveillance is going to be overturned in any way. The right to informational self-determination, hard won thirty years ago with so much verve and pathos, has been fundamentally damaged, and everyone is carrying on pretending nothing happened.

THE PRIVACY PARADOX

The outcome of the German elections calls to mind a phenomenon that scholars have termed the 'privacy paradox'. The paradox lies in the observation that, in surveys and interviews, privacy is always mentioned as being extremely important to respondents, while at the same time this rarely prompts people to do the slightest thing about it.

For a study[15] into the matter, researchers created two fictitious online shops. One of the shops demanded less personal data from their customers, but the DVDs on sale cost one euro more than in the second shop, which wanted to know a lot more about its customers. Almost all users picked the cheaper store. Even when the prices were the same in both shops, only half of the subjects chose the privacy-friendly variety. Apparently, we are not willing to pay a price for privacy. The costs of privacy are virtually zero. Although we keep insisting on how much we care about our data, 'privacy is important!', it obviously is little more than lip service – a mantra that is socially accepted, but devoid of content.

ECHELON AND MOORE'S LAW

That the NSA was eavesdropping on satellite phone connections worldwide was known as early as 2000. Its global network of radio stations and radar domes was called 'Echelon'. The European Parliament called for an investigation, but when the enquiry commission submitted its report on September 5, 2001, it was overshadowed by the events of 9/11 a few days later. Apart from Echelon leaving deep traces in the collective memory of nerd culture, virtually nothing happened – this was a scandal that was to remain without political consequence.

Even 'post-Snowden', no political, technical, or legal solutions to surveillance are forthcoming. On the contrary, surveillance will likely keep on spreading, parallel to the datafication of the world. What was monitored at the time of Echelon was the same as it is today: everything. Only before, 'everything' was less extensive by several orders of magnitude. What *can* be put under surveillance *will* be put under surveillance, i.e. the digitized areas of life. These areas are subject to Moore's Law, meaning that their capacities will double every 18 to 24 months.

The digital tailspin has only just begun. And it will continue to sink into every nook and cranny of daily life, leaving no corner undigitized. So when in ten years' time the latest eavesdropping operations of intelligence are revealed, we might hear of brain scanners, or of sensors tapping into our bloodstreams. Either way, people will shrug it off, or maybe not even that, as their thoughts on the issue will be publicly available anyway.

Our digital lives have been monitored, not just occasionally or recently, but continuously for the past ten years. That means that if total surveillance were as much a risk to personal freedom and individuality as digital rights activists have been suggesting for a long time, no one in the Western hemisphere would be able to feel free or individualistic any more. In other words, the question of whether we can live with total surveillance has already been answered in a way that is by no means hypothetical, but decidedly empirical: yes, we can, and we have been doing so for more than ten years.

---

15 | Alastair R. Beresford, Dorothea Kübler, and Sören Preibusch, 'Unwillingness to Pay for Privacy: A Field Experiment', SFB 649 discussion paper, no. 2011-010, https://www.econstor.eu/bitstream/10419/56724/1/654787352.pdf.

SURVEILLANCE IS A DANGER

Although many of the dramatizations and horror scenarios have turned out to be exaggerated, surveillance – state surveillance in particular – remains a social problem, as it is still a danger to democracy and community. J. Edgar Hoover is a key witness to this effect. The first director of the FBI amassed files on everything and everyone, and had soon collected enough material to blackmail practically all the powers that be in US politics. Hoover was invulnerable, and under his guidance the FBI turned into a state-within-a-state.

Even if it may not be its foremost concern, we can safely assume that the same is true for the NSA. In contrast to the FBI of old, the NSA does not only hold material about US politicians. It has, at least in theory, the ability to compile compromising material about MPs, politicians, and diplomats from all over the world. The intelligence apparatus is indeed a threat to democracy, and globally so.

For many people, surveillance is a very real danger. Spying technology enabled the drone wars in Sudan, Afghanistan, and Pakistan. One false correlation, say you were at the wrong party, or spoke to the wrong people on the phone, and you might find your house in ruins, or worse. Refugees at the borders of the European Union are becoming victims of surveillance on a daily basis. 'Eurosur' is the European border monitoring system for early detection of illegal immigration, consisting of satellite tracking systems, drones, and other recon technology, as well as a scheme for data exchange between the border authorities of the respective member states. Already today, security agencies like Frontex are fighting immigrant streams with high technology.

Even in Germany, it is not too hard to be caught in the crossfire of overzealous officials, especially for politically active individuals. This is what happened to Andrej Holm, an urban sociologist with a focus on gentrification who was held in custody for weeks, and although innocent stayed under observation, along with his entire family, for months. Both the German Federal Criminal Police Office, BKA, and the *Verfassungsschutz*, the Federal Office for the Protection of the Constitution, have time and again tried to infiltrate and demoralize left-wing activist circles with intimidation and investigations.

State surveillance, however, is hardly limited to the intelligence sector. Its repressive traits are far more commonplace than that. Recipients of social benefits in Germany ('Hartz 4'), are bullied with compulsory levies of their personal data. They have to disclose all their property, are required to expect unannounced house calls, and must provide evidence of their efforts to find a job. The constant pressure of being monitored, combined with the threat of losing existing support from the employment agency, is enough to wear anyone down after a while. So there are still many good reasons to be against surveillance, and many specific dangers making it still important to oppose it.

STRATEGIES

The strategies aimed at containing surveillance directly have failed. And while there is the occasional message of success (such as the Court of Justice of the European Union toppling the Data Retention Directive in April 2014), total surveillance is now the default setting – a permanent state that we need to deal with. There are, however, some segments in which surveillance can still be successfully contested.

THE FIGHT AGAINST SURVEILLANCE SHOULD BE A FIGHT AGAINST THE PENAL SYSTEMS

The formula 'surveillance leads to dependency, no surveillance leads to freedom' is no longer accurate in this generalized form. Surveillance does not endanger freedom per se. We are not dealing with an abstract, binary condition that is simply switched on or off. We need to acknowledge that surveillance is a far more concrete relationship, involving at least two parties.

When scandalizing surveillance, we tend to focus mostly on the aspect of observation. We merely ask how pervasive the observation is that we are subjected to. Assessing the threat potential of the NSA, Amazon, or even online advertising companies only on the basis of how much knowledge they have about us is short-sighted, as we overlook the importance of power relations. Surveillance is not identical to power, but power lets observation become surveillance.

Power relations are not in themselves the result of surveillance – they are already in place. On the one hand, surveillance is a symptom of these relations: a certain status or position is required in order to monitor someone in the first place. On the other hand, surveillance can be a tool in this power relationship: it is used to secure and reinforce power. In both cases, the power dynamics were already there. In both cases, this is precisely the point where mere observation turns into systematic surveillance.

Although we are now aware that Google may be forwarding our data to the NSA, we have no qualms in sending private information to friends via Google Mail. To use an analogy, although passersby could notify authorities if they noticed you violating parking rules, you would do it in front of them anyway – but maybe not in front of a police officer. Risk is a concept that is perpetually calculated and recalculated, taking into account the likelihood and intensity of expected punishments. In the same way that we distinguish between a resident and a police officer noticing our illegal parking, we can differentiate between Google collecting our data to show us advertisements, and the Federal Police collecting our data because it suspects us of a crime.

Those with power over me are those who can discipline me. Punishment does not always involve physical violence. Social ostracism, deprivation of love, or even a disparaging look can all have equally disciplining effects on my behavior. It is not until the observers hold me accountable for my actions, that I will experience their observation as a restriction of my liberty as such. The power to punish those not in compliance with the observers' expectations makes all the difference between observation and surveillance.

For that reason, surveillance has only limited relations to privacy. When German writer and anti-surveillance activist Ilija Trojanov was denied entry into the United States in 2013, it was because of his public statements, not because of details from his personal life.[16] In Hamburg, stop-and-frisk police controls have been targeted at people of color in particular, as part of the efforts to monitor the motions of a group of refugees from Lampedusa. This is generally called 'racial profiling'. Skin color is clearly no private matter. The British tourists who made

16 | Ilija Trojanow, 'Willkür und Freiheit', *FAZ*, 1 October 2013, http://www.faz.net/aktuell/feuilleton/buecher/autoren/einreiseverbot-fuer-ilija-trojanow-willkuer-und-freiheit-12599490.html.

a joke on Twitter about wanting to dig up Marilyn Monroe, and who were then interrogated for hours by US border officials,[17] didn't owe their mistreatment to any violations of privacy.

To the observers, it makes little difference whether they call you to account for a public tweet, or for a private email. What matters here is the consequence, not the origin of the information. Even if there was such a thing as an intact private sphere, it could only protect us from repression if we were to retreat into privacy entirely; taking all our potentially objectionable characteristics and opinions with us. If we were to make these opinions public, we would be in trouble anyways. That's not what I call freedom. The LGBT community can try to keep their sexual orientation secret to avoid discrimination, but is that the kind of world we want to live in?

So instead of trying to defend privacy against surveillance, we should be fighting institutionalized punishment. Authoritarian border controls, racist police cohorts, homophobic social structures, inequality in health and welfare systems, and institutional discrimination are the true danger zones in terms of surveillance. Above all, the state itself, with its monopoly on force and its sweeping claims to regulatory authority, is the source of most of the threat scenarios that *do* jeopardize freedom by way of surveillance.

COUNTER-SURVEILLANCE

Trevor Paglen, an artist and activist from New York, practices his very own form of counter-surveillance. Many of his projects make the secret activities of intelligence more tangible. He has located secret agency bases and taken pictures of reconnaissance satellites. He collects rank insignia and documents their iconography, or tracks the routes of CIA aircraft on their way to detention camps. All information he collects he makes publicly available. His work may not grind the maneuvers of the intelligence apparatus to an immediate halt, but it does restrict their freedom of action. The effects of surveillance work the other way around as well: if secret services have reason to fear that their activities could be discovered, recorded, and publicized at any time, they might modify their behavior accordingly.

Surely two of the best examples of the power of transparency are Chelsea Manning and Edward Snowden. Both Snowden and Manning have impressively shown that the information tailspin works towards the side of the whistleblower. No matter how powerful an authority or a nation may be, if its power is founded on secrecy it will remain vulnerable and, if anything, will only become more fragile in the future.

Counter-surveillance has already produced some substantial results in recent cases of abuse of police power in Germany. In 2009, a protester at the annual anti-surveillance march 'Freedom not Fear' in Berlin was beaten up by police. After police officials had simply denied the accusations and claimed that the perpetrators couldn't be identified, they had little left to say in the actual trial when confronted with conclusive evidence in the form of multiple video recordings from different camera perspectives. Two police officers were later charged with assault.

17 | Rob Beschizza, 'Tourists Deported from U.S. for Twitter Jokes (Updated)', *Boingboing*, 30 January 2012, http://boingboing.net/2012/01/30/brits-deported-from-u-s-for-t.html.

In July 2013, criminal charges against Lothar König, a German anti-fascist activist and vicar, were finally dropped. He had been accused of inciting unrest and violating public peace during a demonstration in Dresden. But again, videos from the event surfaced in the course of the trial, severely contradicting the representation of events by the police. Today, Lothar König is a free man again.

We have long perceived data collection as evil, because it is by way of data that we arouse suspicion. Data can incriminate us, and even take us to jail. But this is only one side of the story. We have a limited perspective on data precisely because, for the longest time, data processing had been the exclusive domain of powerful institutions – the state and big businesses. But today that is no longer the case: for the past few years, we have all been collecting, sharing, and processing more and more data, and every day, we collect a little more.

In its most radical form, this trend is called *sousveillance*. The expression was coined by US researcher and inventor Steve Mann, who for the past 36 years has been experimenting with wearable gadgets in order to continuously record his sensory perceptions. He was the prototypical Google Glass user, as it were, long before Google even existed. The term *sousveillance* is derived from the French word 'sous', for 'under' – it describes a way of watching the watchmen, bottom-up.

Thanks to recording equipment getting smaller and less expensive, *sousveillance* had already become an anti-surveillance strategy before the launch of Google Glass. In 2007, police forces in Quebec, Canada, underwent structural reforms after a video on YouTube had exposed plainclothes police officers mingling with the crowd, intent on escalating a demonstration as 'agents provocateurs'. Another video, showing UCLA students being tasered by Los Angeles police without any prior provocation, had similar political repercussions. Likewise, the #OccupyWallStreet protest movement notably amplified in traction and popularity immediately after a number of videos and photographs documenting police violence against the movement began circulating online.

POST-PRIVACY: TRANSPARENCY AS A STOIC EXERCISE

In his book *Post-Privacy: Prima leben ohne Privatsphäre* (*Post-Privacy: Living just Fine Without Privacy*),[18] Christian Heller embraces an even more radical strategy. He argues that it is time to say goodbye to privacy altogether and to embrace the inevitable: transparency. He highlights, amongst other points, the fact that privacy as we know it today is a relatively new form of coexistence, and one that has not only been advantageous. The private sphere has, for the longest time, been the place of the oppression of women, for example. Contrast this with the gay rights movements, which were among the first to show how social progress can be achieved by making ultimately personal information public. Since we are unable to halt technological progress, we'd better get used to the idea of total transparency, says Heller.

18 | Christian Heller, *Post-Privacy*.

Heller himself acts out this idea in practice. He documents all of his daily routines, his finances, and large amounts of highly personal information in a publicly accessible wiki.[19] It is easy to dismiss this as a self-indulgent discovery trip, but Heller is undeniably radicalizing an issue that has become the norm, in social networks anyway, namely the fact that formerly private matters are explicitly being made public.

Unlike many Facebook users, however, Heller doesn't deceive himself. He is highly aware of the fact that his data can be used and abused, by anyone, at any time, for any purpose. In this sense, post-privacy as a strategy complies well with Nassim Nicholas Taleb's dictum of antifragility. Post-privacy is a practical exercise in stoicism: basing your assumptions on the worst case scenario – in this case, that all information is public by default – will not give you a false sense of security, but rather will allow you to make plans in such a way that, should this worst case actually occur, you will not be confronted with unsolvable problems. If you keep in mind that all data is accessible, in one way or another, this can actually reduce anxiety – one of the more negative effects of surveillance.

THERE IS NO MORE PRIVACY, ONLY ENCRYPTION

'Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on,'[20] Edward Snowden said in a Q&A session organized by *The Guardian*. Of all the fragile strategies of data control, strong encryption is probably the least objectionable. End-to-end encryption does not require you to trust an external service provider, or even the state, to protect your data. You only need to trust the technology to make sure that nobody can decrypt the information exchanged between you and whoever you're communicating with. The mathematics behind encryption algorithms are still considered to be bulletproof. Even with yet inconceivable supercomputers, it would probably take thousands of years to decipher a single email.

The issue therefore is less about mathematics than about the implementation of encryption software into email programs, servers, or chat clients. Data can be retrieved in plaintext before encryption, or after decryption. There has been a long line of bugs and backdoors purposefully introduced by hackers or intelligence agencies. That makes encryption particularly suitable for those who are willing, and able, to acquire a lot of knowledge and skills. In this sense, it is a very 'elitist' solution. The need to resort to encryption is not something you'd wish for, but if you do have to rely on confidential communication, encryption is probably still the best, or maybe the only, way to fashion any semblance of privacy on the internet.

19 | Christian Heller, *PlomWiki*, http://www.plomlompom.de/PlomWiki/.

20 | Edward Snowden, 'NSA Whistleblower Answers Reader Questions', *The Guardian*, 17 June 2013, http://www.theguardian.com/world/2013/jun/17/edward-snowden-nsa-files-whistleblower.

Rule 3: Knowing Is Asking the Right Questions

Proposition: In the Old Game, it was important who was storing which information and to what purpose. But what counts in the New Game, by that measure, is how information is retrieved. This shift of focus does not only change our attitude towards knowledge, but also touches on the power structures inherent in any kind of knowledge.

A card designed by US media artist Evan Roth shows the Google landing page, with the words 'bad ass mother fucker' typed into the search field. A mouse pointer is pointing to the 'I'm Feeling Lucky' button, the Google feature that takes users directly to the website that comes up as the first result of a search. The card is essentially a set of instructions in the shape of an image. If you follow the instructions and enter 'bad ass mother fucker' on Google, it will take you directly to Evan Roth's website.[21]

Roth concisely directs attention to the ways in which the public changes in times of the ubiquitous query. Assigning the term 'bad ass mother fucker' to the artist only happens when external observers actively search for the term. The more people follow the instructions and look up 'bad ass mother fucker', the more intimately Roth's name becomes linked to the phrase in Google's algorithms. Of course, Roth primed his own website in advance in such a way that it would appear at the top of Google's list when queried for that particular expression – a practice commonly known as SEO, or search engine optimization.

What is most interesting though, is that Roth does not participate in this process of attribution himself. Because who would want to call themselves a 'bad ass mother fucker'? But by taking this detour, via the Google algorithm and finally, via the Google searcher, this connection becomes one that needs to be maintained and reanimated every time.

Roth's work is a reflection on us – the audience. We are the ones who are meant to perform a particular Google search, thereby feasibly fabricating this particular reality ourselves. The reality of a search engine query contains a very specific notion of 'public'. This is not the 'public' on the street, nor the 'public' of the tabloids. Instead, there are many coinciding publics, ephemeral public spheres that pop up momentarily, connecting any individual with a question to a search result page. These *query publics* don't generate an 'audience' in a conventional sense – rather, it is the audience that is creating query publics of its own.

Our world presents itself, more and more, in the shape of a question. Nowadays, knowledge is rarely structured through inscribing, prescribing, or ascribing activities (many of these are now automated), but rather, through the query. We are constantly making enquiries of Google, of Wikipedia, of YouTube. On our personal computers, the query is slowly surpassing the structure of the file system.

But the question goes even deeper. The query determines what sort of advertising we get to see, and gives us recommendations on what to buy on Amazon. We can see the query at

21 | Evan Roth, http://www.evan-roth.com/about.

work every time we load our personal default settings on any of our online services. Whenever content is personalized and tailored to our needs, we have been recognized and used as a query ourselves. Everywhere we go on the internet, advertising sales companies turn us into queries in one of hundreds of databases. Scientists exploring the world around them use increasingly complex queries on growing amounts of information and call that 'Big Data'. Then they present whatever they found out in their query reality: about dark matter or traffic jams or the climate or the brain. Or about us.

DISTRIBUTED REALITIES

In our Facebook timelines, there is a query pre-selecting the news of the day for us. On Twitter, all the tweets from all the users that we follow are displayed in a single chronological news stream. We have configured our own queries by actively selecting those whose contributions to our reality we value. Today, knowledge means that our Facebook friends and Twitter followers explain the world to us, in their terms.

My Twitter network is as distinct as my fingerprint, and my perceived query reality, by extension, is equally unique. This agglomerate of distributed realities is composed of the status updates of all those personally selected accounts, all those far-flung reality seeders. They share their realities with me, and I aggregate them into my personal query.

THE FILTER BUBBLE

The first to point out possible dangers of the query public was Eli Pariser. In his book *The Filter Bubble* he argues that our notion of reality is increasingly determined by algorithmically filtered content, and explains why he sees this as a threat. Google has become so highly personalized, he states, that no two people would ever get the same list of results for the same query.[22]

Pariser finds these distributed realities problematic. He assumes that we will only follow people with whom we entertain similar worldviews. This selectivity threatens to lead to self-affirmative echo chambers, reinforcing individual standpoints instead of challenging them. So filter bubbles will tend to preserve your own point of view, and insulate you from other opinions. According to Pariser, this undermines the collective process of public debate that is central to any functioning democracy.

However, being confronted with the opinions of others was arguably never a matter of free choice, but a matter of circumstance. Through the query, it has never been easier to connect with like-minded peers from all over the world, and at the same time, disconnect from opinions that you reject. This can justifiably be described as a new form of self-determination. And who has the right to call this new autonomy into question? Or, in other words, to what extent is democracy entitled to the attention of its citizens?

---

22 | Eli Pariser, *The Filter Bubble: What the Internet Is Hiding from You*, New York: Penguin Press, 2011.

Also, bonding with others over particular shared interests does not imply that you won't be faced with more remote ideas and convictions in other areas. Just because I share someone's interest in robots, doesn't mean we have to agree on environmental policies. And just because someone shares interesting links on economics, doesn't mean that I share their sense of humor. Query reality is much more diverse than that: you can configure your filter bubbles so that they provide you with a whole range of unknown, surprising, intellectually and ideologically challenging realities, making it almost impossible *not* to expand your horizon at least once a week. In fact, today, a much greater variety of thought is accessible than ever was possible in the old media world (which itself has only ever served as a filter bubble – the filter bubble of the mainstream), and we can make far more autonomous decisions about it.

Pariser's critique of the lack of algorithmic transparency in personalized services like Facebook is understandable. Creating your own filter bubble is one thing, but a filter that users can only partially influence, or don't notice at all, is an entirely different matter. You can hardly call it self-determination if your demand for information is left up to mechanisms you cannot control.

STRATEGIES

There is no better tool for organizing knowledge than the query. This is true for a range of distributed realities, from newsfeeds to search engines to Big Data. However, we need strategies that can deal with new threats, and make the great potential of the query visible at the same time.

CIVILIAN AND ACTIVIST BIG DATA

In the US, data analysis has long been used to understand (and combat) poverty and inequality. Roland Fryer and Steven Levitt, for example, used extensive data analysis to show that differences in school test scores between ethnic groups had social causes, and no biological foundation – a common racist misconception.[23]

In 2011, it was revealed that Apple Inc. had, for 18 months, contested the release of US Department of Labor data on workforce diversity in California. Apple was harshly criticized by civil rights groups for refusing to disclose information on the ethnic composition of its staff.[24] Imagine for a moment that a large German company would come up with the idea of storing an attribute like 'race' in employee files, and would then pass this data on to the state. The public outrage in Germany would be unprecedented. In the US, exactly the opposite is a cause for concern. Arguably, without data and its analysis, problems like lack of diversity and similar 'invisible' issues are more easily overlooked. That is precisely what is happening in Europe.

---

23 | Roland G. Fryer and Steven D. Levitt, 'Understanding the Black-White Test Score Gap in the First Two Years of School', *Review of Economics and Statistics*, Vol. 86.2 (2004); Roland G. Fryer and Steven D. Levitt, 'Testing for Racial Differences in the Mental Ability of Young Children', *National Bureau of Economic Research*, Working Paper No. 12066, 2006.

24 | Ryan Tante, 'Apple Hides How White It Is', *Gawker*, 9 November 2011, http://gawker.com/5858020/apple-hides-how-white-it-is.

Costanza Hermanin and Angelina Atanasova criticize exactly this point in their article 'Making "Big Data" Work for Equality'.[25] Especially in Europe, there is very little public data on the effects of everyday racism and ableism in the labor market, which, they argue, makes it very difficult to compare diversity data from Europe with data from the US. With their 'Equality Data Initiative', the authors have tried to contend these policies, but they are regularly met with resistance. Privacy, of course, serves as the main counter-argument.

Jane R. Yakowitz Bambauer points out that it is society itself that suffers the most from restrictive data management. In her paper 'Tragedy of the Data Commons'[26] she highlights the fact that open data is a major source of social welfare. With all the restrictive data protection rules limiting this source, she argues that the issue bears similarity to the famous 'Tragedy of the Commons': the problem of selfish participants overexploiting a common good. Her implicit conclusion is that data reluctance is somewhat egoistic behavior.

Germany's Open Data City[27] is one of the few positive examples; a trailblazer in harnessing the political power of data analysis. This small, Berlin-based company mostly offers data processing for German news media, thereby giving the topics discussed a greater range and political impact. One of their first great successes was the visualization of mobile phone connection data belonging to the German *Grünen* politician Malte Spitz, which he had obtained by suing his telephone provider Deutsche Telekom.[28] Using interactive graphics, Open Data City was able to show the quantity of detailed information on the politician's behavior this data might yield. Their mash-up map makes the seemingly abstract dangers involved in government-side data retention all the more visible. You can track Spitz' movements through Germany, for instance, and see any phone call he made in the meantime.

Another example is Open Data City's interactive 'Secret War' map.[29] For this project, they collaborated with German public broadcaster NDR and major newspaper *Süddeutsche Zeitung*. The 'Secret War' project maps the locations of secret CIA, NSA, and BND sites and gives further information on clandestine activities. You can follow prisoner transports, drone flights, and other covert operations launched from specified locations in Germany.

There is still more than enough room for projects like this. Data analysis should be encouraged beyond the economic and academic sphere, and in the activist sphere in particular. It is important to reduce misgivings and increase practical knowledge about this. Key algorithms like MapReduce and database programs like Hadoop are available as open source software, thus affordable for all. At a professional level, hardware costs are indeed considerable, but even with regular hardware you can achieve some impressive results.

---

25 | Costanza Hermanin and Angelina Atanasova, 'Making "Big Data" Work for Equality', *Open Society Foundations*, 9 September 2013, http://www.opensocietyfoundations.org/voices/making-big-data-work-equality-0.

26 | Jane R. Bambauer, 'Tragedy of the Data Commons', *Harvard Journal of Law and Technology*, Vol. 25 (2011), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1789749.

27 | OpenDataCity, https://opendatacity.de.

28 | For the original OpenDataCity project, 'Verräterisches Handy', see: https://opendatacity.de/project/verraeterisches-handy/. For an English version, see: 'Tell-All Telephone', *Zeit Online*, March 2011, http://www.zeit.de/datenschutz/malte-spitz-data-retention.

29 | OpenDataCity, 'Geheimer Krieg', https://opendatacity.de/project/geheimer-krieg-2/.

FILTER SOVEREIGNTY AS SELF-DETERMINATION

Previously, a range of factors such as geography, political affiliations, socio-economic background, language, or financial means, determined which information we came into contact with. Today, most of these factors have been mitigated, and it is possible, at least theoretically, to provide everyone with all kinds of information. Today we can simply choose the information most relevant to us from an almost infinite realm of data streams. In that sense, filter bubbles are the expression of this new form of self-determination, facilitated by technology – an illustration of our right to reduce the complexity of the world according to our own criteria, and to interpret it correspondingly.

In Germany, with its freedom of information laws, a comparable legal right already exists. Article 5 of the German Constitution distinguishes *positive* freedom of information – the right to inform oneself 'from generally accessible information sources without hindrance' – from *negative* freedom of information, which is meant to protect oneself from 'inescapably obtrusive' information.

The query, by way of technology, enhances the potential of both the positive and negative variants of freedom of information. This extended, 'queryological' approach to self-determination is what I call *filter sovereignty*. Filter sovereignty is the right to query, the right to filter content, the right to use public data, and the right to ward off intrusive or unwanted information. Positive filter sovereignty is the right to analyze all information sources through personal queries, while negative filter sovereignty allows us to opt out of certain sources, again using our own filters. In this sense, the filter bubble that you construct on Twitter by actively following accounts, is far more autonomous than Facebook's more obscure news stream. In terms of filter sovereignty, more transparency certainly wouldn't hurt Facebook.

The query, as a driver of the digital tailspin, will keep increasing in importance, and so will the potential of filter sovereignty. Since we can assume that the power of the query will only increase over the next years, filter sovereignty is becoming a core strategy of antifragility. *Kontrollverlust* won't impair this in any way: on the contrary, it will only further enhance the reach and prevalence of autonomous filtering strategies. This is where our most pessimistic predictions regarding informational self-determination meet the more positive potentials of informational freedom. To choose filter sovereignty is to leave the sinking ship of privacy and construct a society based on a form of self-determination that is reinforced, not weakened, by *Kontrollverlust*.

Rule 4:
Organization and Conflict for Free

Proposition: The loss of control over information is also a means of gaining control through communication. In the New Game, the query makes networking, transparency, and organization simpler and cheaper than ever before. This has some benefits, but also brings new problems.

Nicole von Horst was only venting her anger when tweeting in January 2013: 'The doctor who patted my bum when I was in hospital after a suicide attempt.' It was past one o'clock at night, so most of her Twitter followers were already asleep. Still, it struck a nerve. There had been some previous discussions on the German web about everyday sexism. An article by Maike Hank on the *Kleinerdrei* blog[30] spoke of women's experiences with sexism in public, and an essay by journalist Annett Meiritz[31] dissected the misogyny she had encountered in the German Pirate Party. These were followed by a *Stern* magazine article by Laura Himmelreich, where she described some of the inappropriate remarks Rainer Brüderle, former head of the German liberal party FDP, had made.[32] So the everyday sexism topic was already in the air when von Horst posted her tweet, at which point blogger Anne Wizorek came up with the idea to collect these experiences under the hashtag #aufschrei ('outcry').[33]

During the night the gust of wind from that little tweet became a storm, and the storm became a hurricane. Within the next 48 hours 250,000 tweets rolled in, all speaking of very personal experiences with everyday sexism, from sexual harassment to gender discrimination at work, all labeled with the #aufschrei hashtag. Suddenly, #aufschrei was everywhere. For a few days, everyday sexism was as visible as it is ubiquitous.

Sexism is not a major news event. It's 'no big deal', as the victims who suffer from it every day keep telling themselves. Accordingly, the mass media almost never give the issue any attention. As a topic, sexism was perhaps just waiting for the right medium – one that has enough room for smaller stories, for all those moments of everyday oppression and humiliation. Like the internet itself, sexism is an event that is decentralized, dispersed far and wide, and in a way, 'everywhere at once'. On Twitter, all these little waves of everyday sexism added up to the massive flood that was the #aufschrei hashtag.[34]

---

30 | Maike Hank, 'Normal ist das nicht!', *Kleinerdrei*, 24 January 2013, http://kleinerdrei.org/2013/01/normal-ist-das-nicht/.

31 | Annett Meiritz, 'Debatte: Man liest ja so einiges über Sie', *Der Spiegel*, 14 January 2013, http://www.spiegel.de/spiegel/annett-meiritz-ueber-die-frauenfeindlichkeit-in-der-piratenpartei-a-877558.html.

32 | Laura Himmelreich, 'Der Herrenwitz', *Stern*, 1 February 2013, http://mobil.stern.de/politik/deutschland/stern-portraet-ueber-rainer-bruederle-der-herrenwitz-1964668.html.

33 | Nicole von Horst, 'Archäologie von zwei Tagen. Was Brüderle (nicht) mit #aufschrei zu tun hat', *Word Up!*, 24 January 2014, http://literatier.wordpress.com/2014/01/24/archaologie-von-zwei-tagen-was-bruderle-nicht-mit-aufschrei-zu-tun-hat/.

34 | Lars Weiler compiled an archive of all the #aufschrei tweets, available here: '#aufschrei', August 2013, http://aufschrei.konvergenzfehler.de/timeline/.

In the end, the mass media could no longer ignore the topic. The protagonists of the campaign (which had never been a campaign in the first place) were invited to speak on TV talk shows and publish their experiences in newspaper articles. And yet, all these cross-media translations seemed to fail. The essence of #aufschrei was always lost somehow.

In traditional journalism, events are typically broken down to a single narrative, and so most reports reduced the issue to the Rainer Brüderle case. The complexity of the wide range of experiences collected on Twitter was just not representable within the logic of mass media. Mass media can only *reduce* complexity, while the query (a hashtag is nothing else) manages to display the enormous, accumulated impact, as well as the distinctiveness of every individual experience. Twitter accommodates this by providing two different queries onto the same object: one is the query on someone's profile, where I can read a tweet in the context of their Twitter personality, as a unique personal experience; the other is the hashtag query, where I can, for example, read the same tweet in the context of all the other #aufschrei tweets, as part of a massive social disaster.

It is noteworthy that the #aufschrei query not only connected these individual stories, but also connected the people behind the stories. With every single #aufschrei tweet, it became more probable that others would also share their experiences. The cross-links between their tweets also created links on a personal level. In that sense, #aufschrei was a catalyst for the German net feminism movement. The query turned into a real-world structure, giving rise to new friendships, new projects, and most notably, new solidarity.

DON'T PLAN, COORDINATE

In this sense, the query is the flip side of the digital tailspin. It makes possible the representation of the outside world without having to reduce its complexity. It facilitates organization, even while lowering the transaction and communication costs attached, and allows people to network and collaborate without any organizational infrastructure.

One of the most revealing misunderstandings regarding #aufschrei was that it was repeatedly referred to as a 'campaign'. But campaigns are something else altogether: a campaign typically requires some sort of organization or structure – an alliance, an association, or, at the very least, a mailing list. There will be some kind of group structure, so that you can generally tell who is part of a campaign and who isn't. There will be coordination meetings, or nowadays, teleconferences. A campaign will choose a name, and adopt decision-making procedures, be they democratic or autocratic. Participants will make appointments, paint protest signs, inform the media, articulate demands, and eventually start campaigning.

None of this happened with #aufschrei. The only thing participants did here was respond to the query publics with a uniting hashtag; everything else happened of its own accord. The query has fundamentally changed the basic conditions of joint action. Many activities that in the past took a lot of planning in advance, can now be sufficiently coordinated in real time instead. Thanks to the query, this kind of coordination has become so simple, fast, and inexpensive, that it happens almost effortlessly.

An action like #aufschrei is unpredictable. An event like this is not 'planned'; we can merely create the structures that such events may thrive in. By now we should be able to deal with the loss of control; to accept the fact that a movement like this has no 'boss'. The #aufschrei hashtag did not exclude anyone, it did not suppress communication, but rather was a very straightforward way of collecting, aggregating, and coordinating relevant contents.

QUERY WARS AND SHITSTORMS

'Going to Africa. Hope I don't get AIDS… Just kidding. I'm white!' was the last thing PR advisor Justine Sacco posted on Twitter before she boarded her plane. By the time she landed in South Africa, she had become infamous. In the few hours that Sacco was offline during the flight, several news outlets had picked up on her tweet, anti-racism organizations all over the world had publicly complained about her, and her name had been mentioned in more than 30,000 tweets, mostly in highly unflattering terms. In the meantime, she had also lost her job.[35] What happened to Justine Sacco is what the internet likes to call a 'shitstorm'.

This goes to show that opposing ideas, views, ideals, and stories can be connected just as easily and swiftly as shared ones. Antifascists may be confronted with Nazis, feminists with sexists, and racism victims with racists. The query public aggregates dissenting speech just as effectively as affirmative speech.

On Twitter, users have become accustomed to this ambient noise of endless criticism and shitstorms. Every day, some thoughtless or downright malicious statement or action is met with collective criticism. And although the critique itself may be justified, it often seems wildly disproportionate to those on the receiving end. The constant to-and-fro between agreement and disagreement can cause estrangement and breakups in friendships, interest groups, and shared projects alike. The query creates structures (friendships and networks) just as readily as it destroys them, and alienates people from each other just as easily as it aligns them.

This darker aspect of the connective power of the query shows that it is hardly limited to emancipatory or progressive forces, but to their adversaries as well. One of the most reactionary web phenomena is the so-called 'Men's Rights Activists' (or 'Masculinists') scene.[36] United under the flag of their supposed oppression by feminism, these men (and occasionally women) will latch onto any statement or sentiment that a feminist expresses in public. They deliberately try to disrupt feminist discussions, and bully participants with blog comments, Twitter mentions, hate mail, and shitstorms. The methods employed range from sexist slurs to rape threats, all with the declared goal of intimidating feminists, of trying to silence feminism into 'going away' again.

---

35 | Alison Vingiano, 'This Is How A Woman's Offensive Tweet Became The World's Top Story', *Buzzfeed*, 22 December 2013, http://www.buzzfeed.com/alisonvingiano/this-is-how-a-womans-offensive-tweet-became-the-worlds-top-s.

36 | See Robert Claus, 'Maskulismus: Antifeminismus zwischen vermeintlicher Salonfähigkeit und unverhohlenem Frauenhass', July 2014, http://library.fes.de/pdf-files/dialog/10861.pdf.

Racists, conspiracy theorists, and neo-Nazis use the organizational power of the query in similar ways to boost their own agenda. They, too, are aided in finding like-minded comrades, in organizing protests, in building structures and solidarity. This leads to self-referential, parallel worlds that make the inhabitants immune to public opinion and long-established facts.

A storm is brewing that threatens to endanger the freedom of certain groups on the web, more than any intelligence service can. We can presume these hate mobs will only grow stronger in the future. The open web is turning into a no-go zone for more and more people, and so far, we do not have the appropriate mechanisms to deal with this.

STRATEGIES

'Press freedom is the freedom of 200 rich people to express their opinion,' journalist Paul Sethe famously wrote in his letter to the editors of German weekly *Der Spiegel* in 1967.[37] Now, with communication costs plummeting almost to zero, for the first time in history we need to cope with real freedom of expression.

POSITIVE FILTER SOVEREIGNTY

Positive filter sovereignty is the possibility to connect and collaborate with anything and anyone for whatever purpose you like. Even if you do not seize these new opportunities for networking, organization, and coordinated action, *Kontrollverlust* will still catch up with you – it always does; but then there is nothing gained either.

It is all too easy to dismiss the benefits of the cohesive forces of the query as mere consumerism or convenience. Everyday consumption also becomes more effective, faster, and often cheaper, when you can connect with a wide range of services, stores, and individuals at any time. However, positive filter sovereignty extends to the political, cultural, and social operating range of the individual. You can follow people from conflict zones on Twitter for a personal perspective on events beyond your own horizon. You can listen to the lectures of top scientists on YouTube or Coursera, or make contact with political activists from all over the world who are committed to your cause. You can share your insights on political or social matters – or on far more mundane topics – on your blog, Twitter, or Facebook account, and potentially reach a global audience. There are new ways of expressing solidarity, such as innovative campaigns which you can help support and spread. Online petitions can capture prevailing moods and channel them politically. Crowdfunding lets you support the projects that are most important to you; literally enabling you to change the world.

In this sense, the web acts as an expanded consciousness. We can tap into new intellectual, creative, and political resources, and have our ideas criticized, amplified, or enhanced with additional knowledge. On the internet, I am 'larger than myself', engaging with an inestimable amount of additional brain, processing, and storage capacities, which are so unfailingly accessible that I have come to expect their constant availability. Positive filter sovereignty is my mental exoskeleton.

---

37 | Paul Sethe, 'Stimmen verstummt', *DER SPIEGEL*, 40/1967, 25 September 1967, http://www.spiegel.de/spiegel/print/d-46353351.html.

NEGATIVE FILTER SOVEREIGNTY

Negative filter sovereignty is the only antifragile strategy that shields us against hatred and conflict, and it is likely to increase its practical significance. With customized settings, tools, and filters, it is already possible to mute individual trolls and hatemongers. You can block certain Twitter and Facebook accounts if you feel harassed. However, particularly passionate trolls may create a second or even third account, to convey their 'message'. Online platform providers in particular, should be required to develop more effective query settings and blocking tools to reinforce the filter sovereignty of their users.

In the long run, we will need decentralized solutions that are directly installed on end user devices to provide us with more effective protection from unwanted communication. In the future, these solutions will probably not be limited to blocking tools. Ever more complex algorithmic heuristics may be able to prohibit even more specific forms of communication: certain modes of speech and address, or even entire topics, could be anticipated and blocked in advance. The powers of the query are potentially limitless.

MINIMIZING CONFLICT

Anyone who speaks out on the internet can be drawn into an ongoing argument, flame war, or shitstorm.[38] It is not easy to find the right strategy to deal with such a situation, but it helps to be aware of the dynamics of these digitally cued waves of outrage. There is nothing to be gained in such a situation. There is no authority that will end a dispute and declare one of the parties the winner. There are no time limitations, because participants are at each other's communicative disposal at all times. Conflicts therefore always result in losses on both sides. The only question is how high the price is. If the battle has already begun, then it is in the interest of both parties to end the dispute as quickly as possible, regardless of how much the fighters think they are right.

Bernhard Pörksen and Hanne Detel discussed scandals and shitstorms, in the digital world in particular, in their 2012 book *Der entfesselte Skandal* (published in English in 2014 as *The Unleashed Scandal*).[39] One recurring pattern they identified is that of the second-order scandal. This is the scandal that ensues when the actual (first-order) scandal is handled badly. If the implicated parties are obviously lying, trying to wriggle out of things, deleting legitimate criticism, or rendering it invisible in other ways, then all of a sudden the focus is no longer on the scandal itself, but on the misconduct that followed it. Typically, a second-order scandal is even fiercer than its predecessor. It would serve us well to avoid this second level as much as we can, and learn how to deal with criticism.

Following a detailed analysis of various scandals, from WikiLeaks to Tiger Woods' sex addiction to Abu Ghraib, the authors derive a formula that they call the 'Categorical Imperative of the Digital Age': 'Always act in such a way as to make the public effects of your actions appear defensible at all times.' But they immediately follow that up with: 'However, do not expect that it will be of any use.' [40]

---

38 | 'Argument' here is taken to mean an aggressive, emotional and ad hominem conflict. Discussions, even passionate ones, are something else altogether.

39 | Hanne Detel and Bernhard Pörksen, *Der entfesselte Skandal. Das Ende der Kontrolle im digitalen Zeitalter*. Cologne: Herbert von Halem, 2012. English translation: *The Unleashed Scandal: The End of Control in the Digital Age*, Exeter: Imprint Academic, 2014.

40 | Detel and Pörksen, *The Unleashed Scandal,* p. 213.

Rule 5:
You Are the Freedom of the Other

Proposition: Connecting via the query makes social communication structures shift more and more towards end-to-end communication. We need a new information ethics to reflect this change.

The Old Game relied on central mediators: the bank, the library, the authorities, newspapers, corporations, and universities were the ones deciding who was to receive which information and when; the ones making choices about data processing for many others. In the New Game, we can recognize just how patronizing this approach is, and try to conquer it.

Like *Kontrollverlust*, the query public is defined primarily by being unpredictable. A given dataset can back up all sorts of conclusions, depending on what first prompted the query. The as-yet-unknown question is what finally structures the information – the query public is inconceivable in the sense that it always resides in the future.

The least bad attempt to define that grave word 'freedom' is through the distinction between negative and positive freedom. Negative freedom is the 'freedom from' – from violence, starvation, political persecution, etc. This is a sufficiently concrete and coherent definition. If we are victims of circumstance, forced into actions that run counter to our own intentions, we can instantly agree that this is exactly what constitutes a lack or deprivation of freedom.

The concept of 'positive freedom', by comparison, is more difficult to grasp. Positive freedom is the 'freedom to' – to do what wouldn't be possible without extra opportunities. This is commonly paraphrased as 'enabling'. For instance, modern transport technology enables me to travel to the American continent in a matter of hours, spanning a distance not even kings used to be able to conquer. We gain positive freedom by creating new opportunities: expanding our range, increasing our efficiency, or refining our control mechanisms.

It is not primarily the internet that provides these freedoms; we also give them ourselves, to one another. The internet and the query are merely what connect us, end-to-end, or rather 'from one person to the other'. We are the ones generating the news, opinions, texts, and data, which may or may not be useful to others. As we are part of this infrastructure ourselves, we become suppliers of positive freedom to others, and part of their mental exoskeleton. Accordingly, end-to-end communication makes us immediately responsible for the positive freedom of others. This is an ethical constellation that was pioneered by French philosopher Emmanuel Levinas.[41]

Levinas' concept of 'the Other' breaks down the ethics of the community to an ethics of the counterpart. In this sense, Levinas personalized the social sphere, reducing it to its most basic components: the relationship to, and the responsibility for, the Other. At the same time, the Other always retains this somewhat abstract quality of the unknown, unknowable, and un-ownable. The Other is a black swan, an unforeseen event. On these terms, the Other is structurally analogous to *Kontrollverlust* and the query: Levinas' Other is always radically Other, and so the Other will always disrupt any preconceived notion we have of this Otherness. We can never truly know what the Other wants, and this ignorance, accord-

41 | Emmanuel Levinas, *Totalité et Infini: essai sur l'extériorité,* Den Haag: Martinus Nijhoff, 1961.

ing to Levinas, should not only be endured, but in fact gives us responsibility as well; the responsibility being the obligation to *respond*, to answer to the Other.

You are the source, the hub, the database, and the interface of the Other. Your existence, your data, and your offers of communication, co-determine the Other's freedom. Declining to join a certain platform limits the Other's freedom of using it. Not providing an encrypted channel prevents the Other from communicating with you securely. Deleting online content restricts the Other's querying privileges. Finally, suppressing certain kinds of information may constrain the Other in as-yet unknown ways. Pre-emptively responding to the Other should be seen as an act of hospitality.

STRATEGIES

The best strategy for end-to-end communication is to adhere to the ethics of the Other. The Other's filter sovereignty starts with the transmitter.

FILTER SOVEREIGNTY AS INFORMATION ETHICS

When the Prussian politician Friedrich Althoff issued his decree concerning German public libraries in the early 1900s, quite a few librarians were shocked. Althoff was one of the coordinators responsible for a major consolidation of the German library system, the original goal of which was to compile a catalogue with all the books in the associated libraries. To regain control of the vast amounts of material in stock at the time, Althoff was prepared to resort to drastic measures. In his edict, he suggested that the archives be pruned of older dissertations, programs, textbooks, popular literature with no scientific value, nature and travel accounts, and many other items. Most libraries complied with the order, but the university library in Kiel sent the following reply:

> The individual merit of a book is commonly assessed on the grounds of the intellectual sophistication informing it, and since, from this perspective, the scale is unlimited both towards the top and the bottom, its evaluation may well drop to the point of utter worthlessness, and often enough it does. This changes when we acknowledge that every book could just as well be treated as a historical document, in the broadest sense, and as soon as it is part of a library collection, indeed should be treated as such. For a library, every book has at least relative value, which may decrease, increase, or remain the same, and apparently also disappear altogether, even though the issue of value becomes quite clear seen from this angle [...]. So even the most insignificant and trivial of works may increase in value and significance [...]. Therefore, we can regard it as the duty of every public library to preserve [...] the entire collection of books in its totality.[42]

What the defiant librarian aptly indicates here is that the classification of all these books was driven by one specific question, namely whether the information it included was beneficial to readers. But that question could have been posed quite differently: what historical knowledge might we still find hidden in any old pulp novel? Which notions of love or romance could we explore? We simply don't know which other queries could be directed

42 | Nikolaus Wegemann, *Bücherlabyrinthe: Suchen und Finden im alexandrinischen Zeitalter,* Cologne: Böhler, 2000, p. 144. (Translation by the author.)

at the same material. The Other will come along and ask some question we weren't expecting. Hospitality does not mean to fob others off with what is most convenient for us. To be hospitable is to explicitly grant the Other this quality of strangeness and Otherness.

In the German edition of Wikipedia, this contradiction regularly leads to heated debates among the authors. One faction, called the Exclusionists, regularly calls for certain Wikipedia articles with too little 'relevance' to be deleted. The Inclusionists on the other hand, will in case of doubt prefer to keep articles, even when they have no apparent relevance. The fact that, for the query public, relevance is no longer an objective or universal attribute, but more a matter of individual assessment, is something the Exclusionists do not acknowledge. Instead they insist on detailed notability guidelines. If an article does not comply with the rules, it is discarded. As a result, the German Wikipedia tends to include fewer contemporary or pop-culture phenomena than its English counterpart, which follows a more inclusive policy.

The point is the following: if we first no longer need to justify the existence of information due to the affordability of storage space; and second assume that the number of queries applicable to a certain dataset is basically infinite, then there is no legitimate authority that could decide for us just how important or irrelevant, how good or bad, a piece of information is. To this effect, the setup and maintenance of individual queries and filters is the exclusive, radical right of the inquirer.

At the same time, these countless, and hence unpredictable, queries also liberate the sender. The query relieves us of the pressure of meeting expectations – the Other, working with infinite sources and perfectly customized tools, can no longer make demands of the author, neither in the moral-normative, nor the topical or informational sense. The freedom of others to read or not read whatever they like is, at the same time, the freedom of the senders to say whatever they like.

ENCRYPTION AS HOSPITALITY

Encrypted communication also obeys end-to-end principles. Asymmetric encryption generally means that the message you want to send will be encrypted while still on your computer (or mobile phone), and will be decrypted only once it has reached its recipient. End-to-end encrypted data is impossible to decrypt 'along the way', e.g. while on your service provider's email servers. This distinguishes it from so-called 'transport encryption', where a message is encrypted only on its way from the source to the server, and then again between the server and the recipient – on the email server itself, the message will briefly be accessible in unencrypted form. In such a case, authorities can make server operators divulge this unencrypted data with a corresponding court order.

End-to-end encryption will usually employ the *public key* method. A pair of keys is generated using sophisticated mathematical algorithms. You keep the private key to yourself and make the other one public. When you write someone an encrypted email, their approved public key is used to encrypt it. But the recipient will need their own private key to decrypt the message. So you need to provide your public key before someone can send you encrypted messages. A pattern is recognizable here: providing a public key is an act of hospitality towards the Other.

Rule 6:
Platform Control Is Power

Proposition: In the New Game an influential new player has appeared – the platform. Platforms provide the infrastructure that the next society will operate on. In the future, every politically active individual will have to learn to deal with them.

While the state and its centralized institutions are presently under threat to lose a lot of their significance, a new player has already entered the arena: the platform. Platforms are not limited by national boundaries; they essentially just provide access – to individuals and objects, to knowledge and organization. The platform serves as an infrastructure for interaction and coordination, and is home to many powerful query systems. The platform will become the dominant institution in the 'next society'.[43]

Platforms cater to our demands without tying us down: if access to a car is more important to us than owning one, we can carpool. We can rent out our room for a few days because Airbnb and similar outlets make it easy for us to arrange. We can trade unwanted items on Ebay, where buyers can be found for practically anything. And while Facebook has become an internet identification service of sorts, Twitter serves us the daily news, tailored to our needs, at no cost.

A platform may be centralized, like Facebook, or decentralized, like the internet itself. But even when platforms are centralized, they still provide users with opportunities for decentralized forms of organization. And even when they are decentralized, they will normalize everything and anything they come into contact with. Homogenization and standardization are the platform-typical methods used to connect literally everything with everything else.

The most important feature of these platforms is the unlimited, manifold network effects they can have. We are on Facebook because everyone else is on Facebook. We shop on Amazon because of its sheer inexhaustible stock. We use an Android phone or an iPhone because we favor certain apps that they offer. It's difficult for a messaging service to appeal to us as long as it is not widespread. And Google owes its success partly to the fact that it treats search query data as a form of feedback on how to improve its services.

Network effects are reminiscent of the gravitational forces in a black hole: the more they absorb, the stronger they become. The more people, data, apps, products, or developers connect to a platform, the greater its suction will be. Platforms and network effects are the elephant in the room in the New Game. They are already ubiquitous, already powerful – and scarcely regulated. They are on the course of undermining the authority of the state because unlike nation states, platforms reach into all areas of our lives. We make ourselves dependent on them quite voluntarily. But if we shun them, we will only hurt ourselves in the end. We are ensnared all the more by their usefulness: this is the 'lock-in syndrome'.

Meanwhile, platform operators are already turning their power into money. This is not as easy as it may seem. Be it advertising, paywalls, or information brokerage, before you

43 | A term coined by Peter Drucker and applied to the information society by German sociologist Dirk Baecker.

can attach a price tag to something, you first need to control it. So platforms are striving to regain centralized oversight. They claim to be the only ones offering this or that form of access, and apparently we are prepared to grant them this exclusivity again and again.

The platform is here to stay, and so is the normative force of its reality, which we are now permanently subjected to – at least until the next platform comes along to replace the old one. But that will only defer the problem again. The strategies to deal with the platform will therefore have to be political in their very nature.

STRATEGIES

In the Old Game, the centers of power had built-in 'checks and balances', and provided interfaces for citizen intervention or participation. This had not always been the case; indeed, it was hard earned over centuries. Platforms have none of these internal control mechanisms, and apparently do not consider them necessary. We need strategies that enable us to fence in the power of the platforms and involve users in decision-making.

PLATFORM LOBBYISM

When in 2009 Facebook tried to change its terms of service to such an extent that all users would grant the platform unlimited exploitation rights to content they had shared, protests began to form. A Facebook group, 'People Against the New Terms of Service (TOS)', was founded, which attracted 17,000 members overnight and rapidly grew up to 65,000, at which point Facebook felt compelled to respond in a blog post.[44] Finally, Facebook surrendered and retracted the changes. Facebook has since created the 'Facebook Bill of Rights and Responsibilities' group as a forum to discuss their own business conduct with users.

In his 1970 essay entitled 'Exit, Voice, and Loyalty',[45] the economist Albert O. Hirschman examined the options available to dissatisfied members of a group. They can leave the group ('exit'), or speak out ('voice'). Both options come at a certain price, so there will have to be some kind of trade-off. Hirschman, at that time, was obviously not thinking of social networks, but of companies, clubs, and political parties, where abandonment could entail the loss of employment, loss of political agency, or loss of access to certain localities. This is perfectly valid for platforms too. The cost of leaving a platform is largely determined by the strength of its network effects. Quitting Facebook can literally mean you lose the most important channel to connect with your friends. Still, many respond to this kind of criticism of Facebook, Google, or Twitter with only a succinct: 'Well, you don't *have* to join…' Compared to 'exit' 'voice' is a more political alternative. Speaking out about injustice from within the platform can be just as efficient a way of addressing, and redressing, common grievances. Besides, the 'voice' option will become more and more relevant as 'exit' costs continue to rise.

Platforms, in this contemporary sense, are exceedingly political in nature. We depend on them in many respects, and are fooling ourselves if we pretend they are just another ran-

---

44 | 'On Facebook, People Own and Control Their Information', 16 February 2009, https://www.facebook.com/notes/facebook/on-facebook-people-own-and-control-their-information/54434097130.

45 | Albert O. Hirschman, *Exit, Voice, and Loyalty: Responses to Decline in Firms, Organizations, and States*, Cambridge, MA: Harvard University Press, 1970.

dom product. Today, it should be impossible to think about politics while simultaneously ignoring the platform. At some point, platforms will have no choice but to assume more responsibility and engage in political dialogue with, at the very least, their users.

The power of the platform is much needed in order to deal with the waves of online hate speech that await us (see Rule 4). We should urge platforms to protect us from illegitimate third-party interests and unlawful interception from secret services, or even states. Managing user rights, transparency, and accountability in decision-making – including structural changes to the platform, or installing user committees for community management – are the things that civil society should be demanding from its platforms. We also need to make sure that they are not abusing their powers.

A number of civil-society internet policy organizations are well established already today: Digitale Gesellschaft in Germany, the Electronic Frontier Foundation in the United States, and the European Digital Rights Initiative (EDRi) at the European level, to name but a few. These NGOs are lobbying for a free and open web, talking to governments and parliaments, and arranging highly visible publicity campaigns. Even so, it is time for the representatives of digital civil society to direct their attention not only to the states, but also to platform operators.

There are signs that this is happening. The aforementioned Facebook group, 'Facebook Bill of Rights and Responsibilities', is one example. Twitter is increasingly forced to respond to users' wishes, following a wave of complaints against the company's laissez-faire attitude to online harassment. Projects like 'Europe Vs. Facebook', initiated by Max Schrempp from Austria, try to hold platform operators responsible by invoking state regulation. They are therefore still operating within the framework of the Old Game. Occasionally this may work, but it will not be a promising strategy in the long term. We will have to tie civil society directly to the processes and decisions of platform operators. It is time for platform lobbyism.

PLATFORM NEUTRALITY

Network neutrality calls for service providers to not abuse their position as access suppliers, and to treat all data in the same way; thus trying to neutralize the providers' claim to control. In a similar way, we can discuss the need for a generalized version of this demand, namely platform neutrality.

Platform neutrality identifies the infrastructure that is important for enabling social interaction, and attempts to provide non-discriminatory access to and use of it. A neutral infrastructure is a prerequisite for the equality of all participants – to paraphrase Habermas, it is one of the preconditions of any successful discourse. The ideal setting for any speech act is one where everyone has equal chances of initiating and participating in dialogue, equal chances of interpretation and argumentation, and indeed, where everyone is free of domination.

Some caution is required, however. The concept of neutrality has a few pitfalls, as the inventor of the term 'network neutrality', Tim Wu, has pointed out himself. In his 2003

paper 'Network Neutrality, Broadband Discrimination',[46] Wu illustrates the problem by comparing it to one of the most basic claims of democracy: 'All men may vote.' In this claim for equal political participation, we have conveniently overlooked the fact that 'all' was a predefined (and discriminating) notion already. That women were excluded here was not stated explicitly – 'men' could mean both males and humans at the time – but the exclusion of women was accepted as normal.

Whenever we speak of 'neutrality', we run the risk of repeating this mistake. Wu demonstrates that net neutrality falls into the same trap with the following example. 'Best Effort Delivery' is endorsed by many advocates as being the closest thing to actual net neutrality. It means that data packets are delivered and routed as quickly as possible and without making distinctions between the types of data transmitted. This is roughly the way the internet has been working so far, i.e. without any intervention. However, today we have applications that are popular in present-day network management and that call for faster reaction times. Coordinating multi-user games, online phone calls, or remote IT maintenance services, all require a particularly short response time, or as the techies say, *latency*. Such processes will not be well served in an internet that is merely 'best effort'.

Those demanding net neutrality often assume that the current state of the web is already neutral. But that is rarely the case. Today, no one would say, 'All men may vote', but perhaps 'All citizens may vote'. Even that is tricky: take for example the fact that in Germany, residents without a German passport still don't have the right to vote, despite living in the same community. Similarly, we can be as strict as we like in enforcing net neutrality, while other obstacles still remain, like being able to afford an internet connection and a computer, not to mention the different background skills and education needed to use the internet.

Platform neutrality has its problems, but in terms of guidance and long-term goals, it is better than nothing. However, we must not forget the interactive, recursive character of the platform: every platform is based on another platform, so keeping just one of them neutral is not going to solve the issue.

The end user perspective that Tim Wu highlighted for net neutrality is just as relevant for platform neutrality. Platform neutrality is what strengthens the end points – that is, the users. A completely unregulated online community can also cause users to be excluded, albeit indirectly. In online spaces that are full of hate, racism, and sexism, for instance, certain user groups will not feel at home and will disappear quickly or not show up in the first place.

Platform neutrality, for that reason, may even mean that we encourage platforms to implement unequal measures, to compensate for certain imbalances on other levels. Quota systems, or outlawing certain behaviors and modes of expression, for instance, can lead to *more* platform neutrality in some cases than an unmoderated space could provide. What is important is that these processes exacting centralized control are formalized and take place transparently. Platform neutrality, as a political claim directed at Twitter, Facebook, Google, and the like, must also mean that they disclose the criteria by which they are exerting this control.

---

46 | Wu, Tim. 'Network Neutrality, Broadband Discrimination', *Journal of Telecommunications and High Technology Law*, Vol. 2 (2003), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=388863.

MULTIHOMING

As the name implies, multihoming means that whenever possible, applications, services, or data resources are not made available on only one platform, but on several. If there is a certain chat app I want to use that only works on the iPhone, then the iPhone platform is imprisoning me. In this case, the lock-in effect can be alleviated simply by making the same app available for Android phones too. Multihoming is a strategy to make users less dependent on individual platforms.

But because different platforms are often technically incompatible, multihoming can be quite difficult to achieve. Even if an application works on one other platform, this has little influence on general lock-in or other network effects. The question of ethics remains if we recall Rule 5: 'You are the freedom of the Other'. Offering an app on multiple platforms is similar to providing different contact options like Facebook, WhatsApp, and Google+ simultaneously: by doing that, we can increase the freedom of all the others who may want to connect with us. Whether you are a developer, vendor of products, provider of services, or an end user, it makes sense to practice multihoming wherever you can.

DECENTRALIZED PLATFORMS

The most effective way of ridding ourselves of platform dependency is building decentralized platforms. These distributed systems are not controlled by one central authority, but instead arise from many different, but compatible instances. Take email, for example: email works precisely because all the different email providers make servers available that can communicate with one another over the same protocol, SMTP (Simple Mail Transfer Protocol). The web basically consists of nothing more than a protocol (HTTP, or Hypertext Transfer Protocol) and a descriptive language for the actual contents (HTML, or Hypertext Markup Language). Even the internet itself is a conglomeration of a few loose standards (especially TCP / IP – Transmission Control Protocol / Internet Protocol) that everyone can contribute to. You have access to the entire net, independent of which access point you choose. In this sense, distributed platforms are the most radical form of multihoming.

However, it is not easy to find a decentralized substitute to, for example, Facebook. Facebook has a considerable technological advantage that is difficult, but not impossible, to draw level with. Technically speaking, it is quite feasible to recreate the same features in a decentralized form. But the existing network effects remain a difficulty. Platforms like Facebook and Google+ have such a strong gravitational force that it takes a lot of strength to compromise them in the slightest. The attempts at building decentralized platforms have a long history of failure: Status.net wanted to replace Twitter, and Diaspora was poised to become an alternative to Facebook. But why should you join an alternative platform if the people you want to communicate with aren't there?

One of these platforms, however, almost succeeded in deflecting Facebook's power – until Facebook bought it themselves out of sheer necessity. The messaging application WhatsApp doesn't do much more than let users send each other messages, and yet it became a serious threat for Facebook. The app, available for both iPhone and Android, had amassed 450 million users by the time they were purchased, particularly in the teenage target group that is so important to Facebook. Young people use Facebook mainly for its chat functions, and WhatsApp was offering them a real, easy-to-use alternative. Facebook's main

audience was threatening to break away, and so they bought their tiny competitors for the ridiculous sum of 19 billion US Dollars.

Besides its chat feature, WhatsApp has another function that also helped accelerate the platform's success: the app accesses the address book on users' mobile phones – in first versions this even happened without asking – and will then upload it to the WhatsApp servers. In this way, WhatsApp was able to gather millions of address books in a short period of time, and identify with whom users were connected and which of their contacts also used WhatsApp. New users immediately see a list of people they can text right away: a strategic move that has not only brought WhatsApp harsh criticism from privacy advocates, but also incredible success.

The way in which WhatsApp achieved these phenomenal network effects should make anyone dealing with distributed platforms prick their ears. The masses of address books, locally stored on users' mobile phones, are nothing else but one huge, latently pre-existing, decentralized social network. All that WhatsApp did was collect and blend this data, making it serviceable for their users in the first place. In other words, WhatsApp superimposed an application layer onto social networks that were already there.

This brings us to the design flaw in many decentralized approaches, like the social network Diaspora for example. These platforms frequently try to position themselves as a particularly privacy-friendly alternative to Facebook. Their privacy settings will often be strict, thereby shutting their users off from one another. It is difficult, if not impossible, to find friends and contacts on platforms like these. If anything, conceptually these decentralized approaches resemble *anti*-social networks.

WhatsApp, in contrast, got a lot of things right, although it centralized distributed data and in that sense, imprisoned it again: the lock-in effect was back. The same idea could also have been pursued differently: had they kept the address data public, by storing it on several openly accessible servers for instance, then nobody could have locked that data up again in centralized structures. If WhatsApp had used open data, it could have set up its centralized chat service layer on top of the existing decentralized social networks and still have made the data available to third parties.

Decentralized approaches will only work if you keep the data open. Only open data can be centrally queryable and avoid misappropriation at the same time. Just like Google makes the web searchable, but cannot stop others from doing the same; just like the BitTorrent search engine Pirate Bay will track all available torrents, but not exclusively; just like any RSS reader will compile the content of blogs individually, without preventing others from presenting the same content in an entirely different way.

Rule 7:
The State Is Part of the Problem, Not of the Solution

Proposition: In the Old Game, we are accustomed to see ourselves as part of a state that protects us from life's adversities. In the New Game, however, the state itself is affected by the loss of control, and pursues its own agenda. One that runs counter to the interests of civil society.

Just a few months after the first Snowden leaks, the phrase started popping up everywhere: 'We need our own network infrastructures.' Who this 'we' was referring to, however, seemed to oscillate between 'we Germans' and 'we Europeans'.

The conservative daily *FAZ* repeated its calls for a European search engine. It let experts explain how important it was, now more than ever, that Germany, or at least the European Union, would finally build its own net infrastructure. It did not tire of laying at least part of the blame for secret services' surveillance on platform operators like Facebook and Google. Rene Obermann, former head of German telecommunications provider Deutsche Telekom, called for a statutory 'Schengen Routing' in November 2013, mentioning a 'Schengen Cloud' as a set target in the same breath. The 1984 Schengen Agreement was the contractual groundwork that first abolished border controls between different European states, and was later merged with European Union law. But what Obermann was suggesting almost thirty years later was the closing, not the opening of borders. The general idea was to configure European internet routing in such a way that routes of information transfer that left the Schengen territory would be avoided, even if they were cheaper.

At the same time, a number of German email providers, including 1&1, Strato, Web.de, T-Online, Freenet, and GMX, started the 'E-Mail made in Germany' campaign.[47] Providers pledged to exchange email only via encrypted connections. Furthermore, they emphasized the safety benefits that would come from hosting servers only in Germany, thereby subjecting them to German data protection laws. On the German-speaking web, these proposals have since been parodied under the hashtag 'Schlandnet' – a mixture of 'Schland', the football game chant version of 'Deutschland', and 'ChinaNet', a common term for China's highly regulated and monitored national web infrastructure.

This was not too surprising, as the campaign was essentially an easy promotion to give German companies some competitive edge. But the important question of how providers could increase the level of security for their users remained unanswered. It would certainly be welcome for German providers to finally draw level with international safety standards. But an interface called 'Lawful Interception', that grants secret services and other authorities direct access to servers, is still required by law, as in other countries. Of course these all-German email services still include the interception gateway. In this sense, encryption between servers may be well-intentioned, but is of little use as long as intelligence services and others are still given access to stored data.

47 | 'E-Mail made in Germany', https://www.e-mail-made-in-germany.de/.

The most important internet exchange point in Germany is DE-CIX. This network node is where all German and international providers trade their data. Distributed over 18 data centers in Frankfurt, DE-CIX is the biggest internet node worldwide, in terms of traffic. At peak times, traffic reaches rates of up to 3.2 terabytes per second. Essentially, there is hardly any German internet traffic that does *not* pass through here. This is also the place where the Federal Intelligence Service, BND, taps into the wires. According to documents obtained by news magazine *Der Spiegel*, the BND is allowed to record up to 20 percent of total traffic.[48] If you bear in mind that these masses of data can be reduced, for instance by filtering out spam emails, or by storing only the link addresses of data-intensive content like YouTube videos or pornography, but not the content itself, then 20 percent is actually quite a lot. Maybe even everything of importance. And we now know that the BND trades this data on a large scale with its US counterpart, the NSA.

Of course, Germany or the EU could seal itself off in informational terms. But then you would still have to explain why it is preferable to be wiretapped by the German BND or the '*Verfassungsschutz*', rather than by the Americans, especially if the data is made available to the NSA anyway.

What is really being attempted with these 'Schlandnet' approaches is something else. It is an attempt to connect to an old narrative that has little to do with reality today: the good old 'us vs. them' thinking of 20th century nation states, which the world – and the intelligence world in particular – has in fact long outgrown. Since Snowden, it has become common knowledge that the world of intelligence is an immense and finely woven mesh of shared technologies and joint databases, assertively facing the claims to power of individual nation states.

No EU privacy reform, no review of 'Safe Harbor' agreements, no Schengen routing, and no European search engine project, funded with no matter how many billions of euros, will protect us against networks that operate inside Europe, with the blessing of our own governments. The enemy is neither the United States, nor the NSA, nor Google – the enemy is lying in our bed and laughing out loud about our plans to snuggle up alongside it.

The ultimate goal of 'Schlandnet' and its apologists is a re-nationalized, insular European internet, which could thereafter be regulated, finally, with border controls, data retention measures, and automated law enforcement. Of course, all this could then be subjected to even higher volumes of surveillance, which would fit in well with the narrative of the arms race of international intelligence. Is that really what Edward Snowden intended?

ANTI-NET POLITICS

'Schlandnet', data retention, web blocking policies, abolishment of net neutrality, ancillary copyright laws, the 'right to be forgotten', DE-mail, user-unfriendly and unrealistic ideas on protecting minors, tightening copyright laws… Experience has shown that, what in Germany is called '*Netzpolitik*', i.e. internet policymaking, is almost exclusively *anti*-net politics. There's not much use in repeatedly blaming the issue on politicians who are

48 | Ole Reißmann, 'Überwachung: BND soll weitgehenden Zugriff auf Internetverkehr in Deutschland haben', *Spiegel Online*, 13 November 2013, http://www.spiegel.de/netzwelt/netzpolitik/bnd-soll-sich-zugriff-auf-internetverkehr-verschafft-haben-a-933333.html.

supposedly too ignorant, too old, or not tech-savvy enough. It is time to acknowledge that the problem is systemic.

The systematics here are not too hard to pinpoint: boundless networks of people, information, and algorithms are by now questioning the states' claims to power on a daily basis. Like it or not, the state and the internet are so difficult to reconcile structurally, that they are grating against each other more and more violently. The internet and the state have become systemic competitors. Whenever politicians talk about the internet as a 'legal vacuum' (Christian-democratic party CDU) or about the 'primacy of politics' (social-democratic party SPD), they are implicitly raising the systemic question.

Kontrollverlust profoundly affects the state and its institutions, politicians included. That the state keeps its secret services on such a long leash is understandable, as intelligence is the only state-owned tool that is a match for the internet at all. Unlike states themselves, intelligence services can increase their monitoring powers in accordance with Moore's Law, and by way of international collaborations, profit from network effects that are unthinkable for individual nations. It is a dangerous game the state is playing, and its outcome is uncertain. We can be sure of one thing though: in terms of internet politics, the interests of the state contradict those of civil society.

STRATEGIES

Dealing with the state is quite tricky at this stage. The state, we can be sure, still has a lot of power; it can enforce policies within its boundaries, and negotiate new rules at the international level. The state still sees itself as an ambassador of civil society, which isn't entirely wrong, provided your thinking is still defined by national boundaries. It's a fact that we are still greatly dependent on the assertive powers of the state, even while it is the state that has increasingly become the problem. Nation states, with their institutions and stakeholders, are inevitably biased towards the world of geopolitics, which is precisely what needs to be transcended. In strategic terms, we need to strike a balance between working with state power wherever necessary, while promoting its resolution at the same time.

RECOGNIZING INTERESTS

In the New Game all the cards are being reshuffled. Extremely powerful institutions and individuals stand to lose a lot of their authority. It is therefore imperative that we identify the relevant stakeholders and their respective interests.

Newspaper publishers are frantically struggling to survive, and their prolonged crusade against the internet is not in the least altruistic. Hackers tell us that we only need adequate encryption and everything will be fine again, while simultaneously operating companies that sell crypto and security technology. Deutsche Telekom wants us to purchase their services with our dear money, while second-rate German email providers are sensing opportunities to one-up competitors abroad. And the government applauds all these ideas in the interest of business development, safeguarding jobs, or, if nothing else, safeguarding its own powers – and then casually lets still more funds pass for the BND and *Verfassungsschutz*. Surveillance, in this regard, is taking place less between individual states, and more between top and bottom: between the power elites and their populaces.

We'll have to admit that net politics is only possible against the state, not with it. Whether the issue is surveillance, censorship, political transparency, privacy, copyright, or just the emancipatory internet use of civilians, in all these cases the state is something of a natural enemy to civil society. It is time for us to identify ourselves, instead, as part of an international civil society, and to interact and practice solidarity accordingly. An answer to the conflict of states and institutions and their populations can only be found internationally; that is, beyond the policymaking of these institutions or, if necessary, against them. The global protests against ACTA and then TTIP were a good start. They have shown how a global network of activists can form and take joint action, recognizing the international entities who regulate these trade agreements as their political opponent.

THE STATE AS PLATFORM

When the German Pirate Party celebrated its first big success in 2011, and entered the Berlin parliament with 8.9 percent of the votes, many were puzzled about their strange political ideas. Their demands sounded as if they had just combined various unrelated claims of random do-gooders: legalization of drugs, free public transport, voting rights for foreigners, unconditional basic income. All that sounded good enough, somewhat left, and somewhat liberal, but observers were stumped trying to pigeonhole the Pirates within the usual political spectrum in Germany, or even identifying a recognizable political attitude at all.

What these baffled onlookers did not understand at the time was that the party members, who as a group primarily socialized on the internet, regarded public infrastructure as a platform in itself, and hence instinctively aimed at making it platform neutral (see Rule 6). So the free, or more accurately 'ticket-less', public transport system the Pirates proposed, is effectively a non-discriminatory way of moving passengers about, independent of income and intensity of use. Likewise, they demanded that educational resources should be available for all, in equal measures. Suffrage for foreigners who live in Germany implies that the Pirates perceive democracy itself as an infrastructure, hence the advocacy for non-discriminatory, open access to its structures. Even the call for a more consistent separation of church and state can be read as a demand for platform neutrality. Why should the infrastructure of the state favor Christian data packets over Muslim or atheist data packets?

Another of the Pirates' claims, the concept of an 'unconditional basic income', deserves a closer look. If you take the economic foundation needed for an individual to survive to be a *precondition* of the possibility of equal participation, rather than something accomplished with government support only when needed, then the 'unconditional basic income' model becomes mandatory. An unconditional basic income could serve as a non-discriminatory economic platform, where everyone would be at liberty to communicate on equal terms. This makes the entire concept one of the most significant demands for platform neutrality, while also providing a means of strengthening the individual against *Kontrollverlust* by increasing overall robustness.

This line of political thought is not limited to the Pirate Party, but can be found in contemporary internet activism as well. If we are to work with, and around, the state, we have to do exactly the opposite of 'Schlandnet': we need to turn the state into a platform, disempower its centralized control systems, and transform it into an egalitarian infrastructure of social participation.

POST-NATIONALISM

The state is forcing us to rethink net politics, even beyond the net. This calls for another step towards policies that are essentially anti-'Schlandnet' in nature. Instead of re-nationalizing the internet, we need to overcome national boundaries through our networks. If goods and information can flow without any border controls today, why can't people?

If we want to curb the dangers of surveillance by combating the penal system (see Rule 2), then the border of the nation state is exactly the place to start. This is about more than a German author's admittance to the US, or asylum for Edward Snowden. The infamous 'Fortress Europe' is a draconian nightmare of state surveillance, with deadly consequences for thousands of people. Compared to the 23,000 who have died or gone missing on their way to Europe since the year 2000 alone,[49] the Berlin Wall fatalities seem like tragic singular cases.

National boundaries need to be gradually eliminated, immigration controls need to take place according to verifiable international standards, and in the long term, we will need an international human right that protects freedom of movement. It's going to be challenging to discuss this with politicians, who are bound to the nation state by design. Rather, this debate requires a decidedly transnational agenda of a truly global civil society, which is aware of the conflict of interests it has with its own heads of state.

49 | Sylke Gruhnwald and Alice Kohli, 'Die Toten vor Europas Toren', *Neue Zürcher Zeitung*, 2 April 2014, http://www.nzz.ch/aktuell/startseite/die-toten-vor-europas-tueren-1.18272891.

Rule 8:
Data Control Creates Hegemony

Proposition: Any attempts to contain Kontrollverlust will only reinforce the power base of platforms. Data control entails centralized control, and therefore weakens civil society.

In the Old Game, it was often purposeful to enforce data control in order to limit existing powers. Copyright was meant to protect the rights of artists and authors against influential publishers. Privacy was intended to shield civilians from the control exerted by institutions. In the New Game, however, this approach no longer works, and in fact, it may produce exactly the opposite effects.

Copyright enforcement leads to monopolistic platform configurations, imprisoning the creators themselves without further benefit. Data protection requirements give platforms reason to shut themselves off, limiting their interoperability, and reinforcing lock-in effects. Any law aimed at regulating platforms will actually work towards strengthening their power base.

STAKEHOLDERS AGAINST *KONTROLLVERLUST*

Kontrollverlust is actively being opposed on all levels of society. We can identify three drivers, or stakeholders, working against the tailspin. First, we have the platform operators themselves, striving to centralize control in order to protect their business models. Second, there is the state that forces platforms to centralize control, in order to comply with legal requirements. And finally, the users themselves are demanding more centralized control from the platforms they use.

This tendency is quite plainly visible in copyright law. Culture is being turned into a flat rate, with restricted access organized over platforms: the developments are the same, whether it concerns music (Spotify, Pandora), movies and TV series (Watchever, Netflix), or books (Amazon is currently planning a flat rate for e-books). Rights exploiters are also harming themselves in the process of becoming platforms, but first and foremost, they are harming creators. The works of artists remain stuck in digital silos, and alternative usage is ever more rarely permitted, even while the price of cultural goods keeps dropping.

All platforms share exactly the same problem today. They provide communication, culture, or conversation, and the tools to make it happen. So actually, they are designed to leave control up to the end user – and ideally, the platform itself will retreat into the background. But this becomes their exact problem as soon as it comes to delivering advertisements, for example. Maybe users visit sites with a browser that uses ad-blocking extensions, or maybe they have a third party app installed on their phone that only displays content, and not ads. Moreover, if platforms want to establish payment models, they will also be forced to control user access. The first stakeholder of anti-*Kontrollverlust* commands: if you want to make money, you have to control user interactions.

The second stakeholder, the law, also forces platforms into centralizing control: operators have to react to rights violations taking place on their platforms, which in German legal jargon is termed *Störerhaftung* (liability for disturbance). At which point though, is

a certain right violated? Not every case is unambiguous, yet platform operators have to decide in order to be on the safe side of the law. They are required to interfere with communications, pass user data along to law enforcement, or delete and block user profiles entirely. Much of this happens at their own discretion, so platforms are driven into the role of cops.

In fact, converting platforms to informal instances of the law achieves the opposite of what the enemies of the platform intended. This is best illustrated with the 'right to be forgotten', where the idea of filter sovereignty directly collides with the established right to 'informational self-determination'. In mid-2014, the European Court of Justice ruled that, under certain circumstances, people may put in claims to have specific links removed from the indexes of search engines like Google, if these links come up when searching for that person's name. If links that appear there contain content that discredits you, or dates back a long time, you may be entitled to prohibit that this connection shows up in a search.

However, this decidedly reduces the filter sovereignty of millions of other people. And of course, the search engine will still have the 'forgotten' content at its disposal. It has to, otherwise the websites concerned would just be indexed again the next time the search engine's bots crawl it. This, in turn, means that companies like Google have to keep account of a comprehensive hidden index, which explicitly links to content that has been flagged as compromising. Is there any greater power we could afford a company than this?

In the end, the 'right to be forgotten' leads to an alarming intensification of the concentration of power: our increasingly non-transparent queries are subject to filtering, by way of secret lists of things we mustn't know about, and the explicit request for oblivion makes search engines act as prosecutor and judge rolled into one when confronted with ambiguous legal questions. Johannes Masing, judge at the German Federal Constitutional Court, aptly put it this way:

> By making search engine operators responsible for cancellation requests, the decision of the European Court of Justice elevates them to the position of private arbitral authorities, with extensive decision-making powers over network-based communications. The ruling hence threatens to solidify their already considerable power.[50]

Finally, the third stakeholder of anti-*Kontrollverlust* is urging platforms to behave as outright sheriffs when it comes to critical norms and standards. Users understandably have the need for some community management, such as the termination of stalking or harassing accounts. But the privacy requirements that users would like to have enforced against all other users, and even personal acquaintances, are often the basis for legitimizing closed platform structures and centralized control mechanisms. In the United States even more so than in Europe, there is a tendency to expect a 'clean Facebook experience' that doesn't allow, for example, naked female breasts. And in Germany, many users would like to see right-wing sites disappear from view.

---

50 | Johannes Masing, 'RiBVerfG Masing: Vorläufige Einschätzung der "Google-Entscheidung" des EuGH', *iRights*, 14 August 2014, http://irights.info/artikel/ribverfg-masing-vorlaeufige-einschaetzung-der-google-entscheidung-des-eugh/23838. (Author's translation)

Whether we like it or not, in these indeterminate realms of the law in particular, we are using platform operators as a new kind of all-in-one police, court, and prison. In this manner, we authorize them to enforce a platform-based power monopoly that vastly extends their existing powers.

PLATFORM CONTROL AND MANIPULATION

When air travel became a mass market in the 1950s, IBM, together with the US Air Force, had already developed the so-called SAGE system. SAGE was a computerized anti-aircraft defense system that collected data from different radar stations and transmitted it to central locations. Remarkably, SAGE also seemed to have precisely the features that were interesting for booking procedures in civil aviation. So IBM, in cooperation with American Airlines, went on to develop SABRE (Semi-Automated Business Research Environment), a booking system that could transmit data on flight itineraries over long distances, and coordinate and perform seat reservations. This system turned out to be a great success, and travel agents started using it to book flights for various airlines. SABRE can be seen as one of the first digitized networked platforms.

Then it was revealed that the flight reservation algorithms were manipulated in such a way as to favor American Airlines flights. For instance, even if an AA flight was entered into the system later than others, it was displayed at the top of the list – and travel agents tended to mainly notice the topmost entries, just like Google users do today. Additionally, special offers or discounts from competitors were simply censored out of the system. In the US Congress inquiry into the allegations in 1983, Bob Crandall, president of American Airlines, defended these practices saying that having this competitive benefit was legitimate and reasonable 'for having created the system in the first place'.[51]

Hopefully, platform operators today are more aware of the problems that arise from manipulating their queries. Only how do we verify that? Usually we are at the mercy of the platform when it comes to filtering search results. It's an issue that has existed for a long time, as the American Airlines example shows, and not only in theory – it is a problem that has had massive impact on political discourse already.

On August 9, 2014, 18-year-old Michael Brown was shot dead during an altercation with police in Ferguson, Missouri. A police officer on patrol had stopped him because he had dared to walk in the middle of the street instead of the sidewalk. During their argument, the police officer's gun fired from within the vehicle, either intentionally or as a result of the struggle. Brown then fled the scene and was shot six times from behind. Michael Brown was unarmed. And he was black.

A police report for the state of Missouri had already caused some controversy the year before, as it showed that the likelihood of being arrested when stopped by police was twice as high for blacks as it was for whites.[52] Racial profiling by police is all too commonplace in the US; black citizens are regularly put under general suspicion.

---

51 | See Thomas Petzinger, *Hard Landing*, New York: Random House, 1995, p. 272.

52 | Ferguson Police Department, 'Racial Profiling Data/2013', http://ago.mo.gov/VehicleStops/2013/reports/161.pdf.

The next day, the black population of Ferguson in particular assembled for a peaceful vigil and was immediately met by 150 police officers in full riot gear. The atmosphere grew increasingly tense and the situation got out of hand. Riots, looting, and street fights started to take place. On August 11 and 12, police forces began using armored vehicles, stun grenades, smoke-bombs, tear gas, and rubber projectiles against the protesters, escalating the situation even more. Soon the images of Ferguson's police presence enforcing martial law started spreading all over the world, all over the media and, of course, all over the social networks.

But the images didn't spread in the same extent in all social networks. In a blog post published on the news website *Medium*, researcher Zeynep Tufekci, who works on the influence of algorithmic news filters on political power, notes that the events in Ferguson were presented very differently on Facebook than on Twitter.[53] Ferguson had hardly featured in her Facebook stream, while there had been talk of nearly no other subject on Twitter. This clearly wasn't due to the fact that Facebook users were not discussing the issue: it was Facebook's EdgeRank algorithm (used to personalize news feeds according to user preferences) that was apparently blinding out the topic altogether. But algorithmic filtering exists on Twitter as well. The so-called 'Trending Topics' generally highlight the most relevant current issues, preselected accordingly for the country or region. Even in the US list of topics, Ferguson was not 'trending', despite its immense presence.

We don't have to construe any conspiracy in order to admit that there is a problem here. If we consider that platforms are turning into the most important infrastructure for social discourse, then their streamlined queries become a political matter, a critical infrastructure for democratic debate. An infrastructure subject to non-transparent queries, provided by non-transparent companies with tight connections to intelligence services – what could possibly go wrong?

STRATEGIES

Privacy advocates often demand better control of these platforms. But in fact, the opposite is advisable: it is loss of control – *Kontrollverlust* – that should be enforced against the platforms. The future of the platforms, whether they turn into a new form of tyranny or into a new form of self-empowerment for civil society, will be decided on the grounds of the control that we afford them, or expect of them. Only if we grant these platforms as little control over the flow of information as possible, or none at all, will they be able to become a real infrastructure rather than an unrestrained apparatus of power.

That is to say, the informational tailspin is on our side and it calls for Open Data. The platforms will forfeit their power only if their data can be evaluated with various, ideally unlimited, numbers of external queries. They lose the power to exclude users, because those users can publish elsewhere. They lose the power to manipulate queries at will, because users themselves can perform queries on the data and make their own judgments. They lose the power to lock users in, because they can no longer prevent users from parsing their data, forwarding it, and evaluating it in other ways. Open Data is the only way of

53 | Zeynep Tufekci, 'What Happens to #Ferguson Affects Ferguson: Net Neutrality, Algorithmic Filtering and Ferguson', *Medium*, 14 August 2014, https://medium.com/message/ferguson-is-also-a-net-neutrality-issue-6d2f3db51eb0.

escaping the trap that platforms will set otherwise. But this freedom comes at a price. In the long term, we will have to do away with centralized controls on various levels, be it privacy, copyright, community management, or law enforcement.

NO COPYRIGHT

No Copyright is the title of a critical analysis of copyright laws by political scientist Joost Smiers and business economist Marieke van Schijndel.[54] They argue that the monopoly of rights exploiters, legitimized by copyright laws, is what leads to an increasing concentration of the global culture industry, which favors only a few large corporations and the resulting 'blockbuster' culture. The authors make a radical case for the abolition of copyright, in the hope of decentralizing this cultural consolidation.

Many of the political attempts to monitor and control the internet are connected to copyright directly. But trying to reconcile the internet with copyright is like flying a glider through a vacuum: impossible. Nonetheless, this doesn't stop some from trying with force. As long as copyright exists, people with enough money and influence will attempt to repurpose the internet into a control society. In the short term, we have no choice but to use free and open licensing models, thereby at least causing the longest possible detours around copyright, in order to keep these pursuits of power in check. In the long term, we will have to dispose of it altogether.

In view of the available options, we basically have a moral obligation: the internet provides the opportunity to make information instantly and globally accessible for all. This is surely a utopia. Nevertheless, it is a utopia that is hindered not by technical or economic obstacles, but by legal hurdles – copyright restrictions in particular. It is the vision of this opportunity itself that obligates us to pursue it – that is, to abolish all the exclusive distribution rights over information.

The social benefits of the abolition of copyright could be immense. Imagine a network without borders, a global knowledge base without access restrictions, a remix culture without transaction costs – an unrestrained form of creativity that would be fully connective for every thought, every word, and every image, all over the world. Imagine a genuine information society. The chance is definitely there. If the prices for cultural goods continue to decline, this will take the financial pressure out of the copyright debate. This, in turn, will only be encouraged if we file share diligently and distribute our intellectual and creative products under free licenses.

THE RADICAL RIGHT OF THE OTHER

Despite my argument that platforms should, in the short term, be given the role of necessary regulatory authorities (see Rule 7), we must not forget how much power we are endowing them with. In the long term, this strategy can turn into a problem.

Another strategy has already been mentioned several times: filter sovereignty. Unlike the centralized assertive powers of the platform, filter sovereignty is constructed from end-to-end, i.e., achieved in decentralized ways. In the future, we will come to rely on this autono-

54 | Joost Smiers and Marieke van Schijndel, *No Copyright: Vom Machtkampf der Kulturkonzerne um das Urheberrecht. Eine Streitschrift*, Cologne: Alexander, 2012.

my and be empowered to connect with everything and everyone we like, just as we will be able to effectively block out everything and everyone we dislike, for that matter. Presently, such practices are still only developing rudimentarily, and mostly with recourse to centralized platform structures, as, for example, with the blocking and unfollowing mechanisms on Twitter. Technically speaking, however, there is nothing that should stand in the way of an effective, decentralized extension of these filtering tools.

With the increasing influence of the query, filter sovereignty becomes the 'radical right of the Other'. This can be summarized as follows: no one has the right to be read, heard, or acknowledged, just as no one has the right *not* to be read. Which, in practice, means nothing else than the following: all Others, and their respective queries, have the fundamental right to analyze, and ignore, whatever they like. This solution may be radical, and certainly has some side effects that need to be warded off, but the alternative would mean, in the long term, giving in to the immaturity and heteronomy that centralized platforms impose.

RELEASE ALL THE DATA!

In his book *The Transparent Society*,[55] the scientist and author David Brin recounts a fable that I would like to retell in condensed form here:

> There was once a kingdom where most people could not see. Citizens coped with this cheerfully, for it was a gentle land where familiar chores changed little from day to day.
>
> About one person in a hundred did have eyesight. These specialists took care of jobs like policing, shouting directions, or reporting when something new was going on. The sighted ones weren't superior. They acquired vision by eating a certain type of extremely bitter fruit. Everyone else thanked them for undergoing this sacrifice, and so left the task of seeing to professionals. They went on with their routines, confident in a popular old saying: 'A sighted person never lies.'
>
> One day a rumor spread across the kingdom. Shouted directions sometimes sent normal blind people into ditches and occasional harsh laughter was heard. This suggested that some of the sighted were no longer faithfully telling the complete truth.
>
> The news worried the blind subjects of the kingdom. Some kept to their homes. Others banded together in groups, waving sticks and threatening the sighted. One faction suggested blinding everybody, permanently, in order to be sure of true equality – or else setting fires to shroud the land in a smoky haze. 'No one can bully anybody else, if we're all in the dark,' these enthusiasts urged.
>
> Then, one day, a little blind girl had an idea. 'Here,' said the little girl, pushing bitter fruit under the noses of her parents and friends, who squirmed and made sour faces. 'Eat it,' she insisted. 'Stop whining about liars, and see for yourselves.'

55 | David Brin, *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?* Perseus: New York, 1998.

Institutional regulatory instances fail in the face of the platforms' rising powers. We are dependent on the platforms, just as the blind people in the tale are dependent on the sighted. But there is a way out. Only the query can control the query. For that to work, however, the data needs to be open, and so we too, will have to relinquish some control. Sooner or later, we will have to eat the bitter fruit; we will have to open all data up for unguarded aggregation and analysis.

The only way of effectively preventing queries from being manipulated and used against us is by embracing redundancy. If Google really were the only competitor in the search engine sector, we would certainly be well advised to distrust it deeply. Thus far, though, everyone can create an index of the web and organize it at discretion, provided they have the appropriate technical and financial resources. And plenty of them do: Microsoft's Bing, DuckDuckGo, Wolfram Alpha, and many others, work in more or less the same way as Google. Market share in that sense hardly matters, as long as there is the option of cross-checking queries. As long as competing queries can test whether Google is abusing its powers of the query on a grand scale, these powers are at least to some extent contained.

However, in order for these reliability checks to remain in place, data needs to be queryable by everyone. Thanks to the open web, this is still the case. This approach, however, seems to be on the decline: Facebook, and more recently Twitter and other platforms, are increasingly shielding their data from third-party queries. That is the real issue at hand. So instead of demanding more privacy, we should convince platform operators to open up their data. Because the more open the data becomes, and the more queries can be applied to it, the easier it will be to fence in the power of platforms.

Rule 9:
And the Final Boss Is… Us!

Proposition: The biggest adversary of civil society is neither the NSA, nor the platforms, nor the state, but civil society itself. We will have to learn to live together, to address social problems collectively, and to take on a lot more responsibility.

In the Old Game, the individual could rely on the centralized order of the institutions, and would therefore only occasionally be bothered with the complexity of the world. With this frame of reference, it was easy to confuse freedom with the illusion of self-reliance: to be free was to be independent.

With the forfeiture of informational self-determination, this notion of freedom is rapidly losing significance. As the German philosopher Antje Schrupp has repeatedly pointed out, our prevailing concept of freedom is based on a male-dominated ideology of privilege.[56] The illusion of self-reliance can only be maintained if the conditions of this self-reliance are kept invisible. For instance, when housekeeping and childcare were taken care of, the patriarch could assure himself of his own autarchy, turning a blind eye to his wife's work, or his personnel's, without a thought. Even though today we are far beyond patriarchy in its initial form, we still tend to assure ourselves of our autarchy by painstakingly overlooking the infrastructural parameters of our lifestyles, and by taking them as a given. In contrast, the internet reminds us constantly that we are part of a social fabric, and highly dependent on social infrastructures. This prospect is not always pretty, and imposes a responsibility on us that we were previously able to shift on to higher institutions.

If we try to paint a rough picture of the next ten to twenty years, we'll see that neither the intelligence services, the state, nor even the centralized platforms will pose the greatest challenges. The final, end-of-level boss in the New Game is not one of the strong players of the Old Game. Rather it is us, ourselves, who have to take on the challenge of making do without them.

THE FINAL BOSS IS NOT THE STATE

The power of the state is notably decreasing even today, and in matters of internet policy, it has already made itself dispensable as a dialogue partner. State institutions will be increasingly and effectively circumvented in the future, and politicians will accept without objection. The state will not disappear entirely, but fade into the background. Institutionalized politics, meanwhile, is trying to weave the old order into transnational and European-level governance, and can be expected to have some success with this mission. We should be vigilant and careful not to trust the state too much, and if necessary, directly challenge its claims to control. A 'final boss', however, looks a bit different.

THE FINAL BOSS IS NOT THE SECRET SERVICE

The influential status of intelligence today appears to be more or less independent of the state's waning importance. At first glance, secret services appear to be on a drip feed from

56 | Antje Schrupp, 'Über das Müssen', *Bzw-weiterdenken*.be, 13 August 2008, http://www.bzw-weiterdenken.de/2008/08/uber-das-mussen.

their respective governments. But in fact, they have been crafting a global meshwork of largely self-sufficient and self-referential structures which are not going to disappear any time soon. Intelligence has become an international platform of secret knowledge, and in the New Game, espionage will still be playing an important – and probably unpleasant – role. However, the secret services are severely endangered by *Kontrollverlust* themselves, and in such a way that their inner workings and activities are systematically called into question. There is credible evidence that Edward Snowden is not the only whistleblower supplying the public with classified information. Most likely there is a second anonymous source,[57] and some observers already speculate about a third.

NSA, GCHQ, and BND are accumulating greater intelligence and data analysis capacities by the hour, but their modus operandi is fragile. The informational tailspin ensures that now their operations are less undisturbed than before, and the climate of mutual suspicion within their own organizations numbs their efficiency. While intelligence still remains a force to be reckoned with for civil society, it is not its main opponent.

THE FINAL BOSS IS NOT THE PLATFORM

Platforms already have a firm grip on our lives, and this development can be expected to spread even further. In the future, we will arrange virtually everything via the platform. Without question, this will afford them an immense power base. Platforms will continue to expedite concentration and monopolization, and they will continue to do politics by way of exclusion and manipulation. And we will not just approve of this, but actually demand it – and despise them for it at the same time. Platforms are making themselves irreplaceable to us, and our dependency on them will relentlessly force us to accept essentially unacceptable conditions, even though we should try to induce political counter pressure.

But we mustn't be so gullible as to imagine Facebook and Google as the incoming platform rulers of the world. They are merely early insignia of a new paradigm that is only just unfolding. The day we log on to their far more powerful successors, we will find that their current supposed power was a mere joke in comparison.

Of course, there will also be new approaches of decentralization, aimed at dispersing the power of the platform rather than monopolizing it, and promoting inter-operational standards and open source technology. It is to be hoped (and technically quite feasible) that an open, decentralized, 'social network layer' can be developed, as a kind of add-on to the internet. This would then be able to replace a large portion of Facebook's current functionalities and provide a more open kind of access to essential forms of online communication. But we shouldn't be too hopeful in this respect. Centralized, closed source, platform monopolies, with their thirst for profit, will still have more than enough space in the New Game, as long as we don't abolish capitalism in the meantime. They are not going away, because their investment facilities are still greater, their scaling effects stronger, and their innovation and development cycles shorter than what can presently be achieved with common standards and open source.

---

57 | James Bamford, 'The Most Wanted Man in the World', *Wired*, 13 August 2014, http://www.wired.com/2014/08/edward-snowden/.

Platforms are set to become the most important centralized power stations in the near future. But for a 'final boss' they are too volatile, and far too dependent on us in return. After all, their livelihood ultimately depends on how much power we are prepared to grant them.

THE FINAL BOSS IS… US

We are not quite ready yet. Most of us are still stuck firmly in the 20th century and refuse to acknowledge the rules of the New Game. *Kontrollverlust* makes us nervous, and it is due to this anxiety, this loss of familiar routines, that we demand to be shielded from it. And so we call upon the state to protect us: from platforms, from intelligence services, and so on. Then we demand that these same services protect us from other secret services, or from terrorists. And finally, we call upon the platforms to protect us, from one another, from the state, and again, from the secret services.

We are essentially aware of the contradictions in our various claims here, but have internalized these expectations. We have learned that we are asserting our so-called rights to make these demands, but ignore the fact that we are dealing with separate players and conflicting interests. Unfortunately, this approach puts us in jeopardy ourselves: we are encouraging those we fear, and happily relinquishing our tools of self-determination. This strategy is eventually doomed to fail, and at worst may even lead to an uncontainable imbalance of power.

Meanwhile, we are particularly unable to cope even with ourselves. We go along with shitstorms, intent on tormenting each other – hey, it's free of charge. We provoke others, and let ourselves be provoked. We escalate a quarrel here and wage a mock fight there. 'Someone is wrong on the internet!'[58] is our battle cry. We like to display our intolerance of the lifestyles, convictions, cultural backgrounds, and principles of others, and are rarely willing to inform them of our point of view before berating them.

Let's face the facts: digital tools have empowered the individual and civil society. We have all gained more opportunities: to communicate and affiliate with others, to assert our interests, to organize ourselves. Sadly, we seize these opportunities in order to prevent one another from making progress. The NSA may in theory have the power to pressure, intimidate, and terrorize each and every one of us. And this is exactly what happens to a lot of people who are silenced on a daily basis – not at the hands of the NSA, but at the hands of trolls, 'Men's Rights Activists', Nazis, and other misanthropes.

In this respect, the perpetual drama on the web has at least some purpose. Unresolved societal problems are behind almost all of these points of friction – problems that existed before, but were more easily concealed in the Old Game. On the internet, there is always a sufficiently critical mass of people to be found who consider a specific grievance to be outrageous enough to denounce it. Getting them together may be hard work, but it is usually a good solution. Social progress only works this way.

We will carry on hurting each other for a while, until we finally realize that these new digital tools can only cause so much distress because they have given us new means of control. In a word, we have gained powers that we have not yet learned to wield: powers that are

58 | 'Duty Calls', *xkcd*, http://xkcd.com/386/.

inadequately regulated, offer very few effective control mechanisms, and for which we have, so far, barely developed any cultural practices. Our true final boss is our inability to see ourselves as actual beneficiaries of these powers.

STRATEGIES

So how do you fight yourself? Preferably in such a way that you are not too badly mangled in the process. Under the end-to-end paradigm of the New Game, everyone has to take on more responsibility. Otherwise, the others will take over: the platforms, the secret services, the nation states. And that would probably not end well.

POLITICS OF EMPATHY

The liberal / libertarian model of freedom as independence and self-reliance is finished. It may take some time, though, before certain people recover from this insult to humanity and realize that it actually yields a new liberty: the positive freedom of connectivity, interaction, and involvement. Freedom, however, that comes at the price of greater responsibility. In his column 'Connected', the computer scientist and internet scholar Jürgen Geuter writes:

> The Internet is a network, therefore it replicates human coexistence much better than many people care to admit. And the intrinsic value of a network does not lie in the sovereignty and independence of its nodes, but in their connectedness, and the emergent behaviors that result.[59]

As part of a network, we can benefit from these network effects, but then we need to take more responsibility for the network itself. In the New Game, nothing we do is unpolitical anymore. We are role models all the time, for better or for worse. We become politicians ourselves, as soon as we complain about the sorry state of affairs, as soon as we speak out against racism, sexism, or homophobia. But we are also acting as politicians whenever we spread this kind of hostility. The internet is not the regulars' table, we should quit the pub talk and realize that we are already operating in the query public of Others. All of our actions serve as an example, and are, in this sense, inherently political.

The lack of transparency in the Old Game let many of us go about our business unperturbed, despite the massive social problems that surrounded us. Clearly, the internet has not caused hatred and animosity, but it is there that they are most simply represented. And it is from there that this hate will be spouted back at us. In the New Game, it won't matter what you know, but rather what you are willing to learn. Life in the network calls for much more empathy than in the Old Game. In this regard, empathy means the willingness to engage with the views of the Other.

Empathy also implies a willingness to enrich the network with our contributions. Connectivity is not opposed to individuality – instead, our individuality augments the network and is what ultimately makes it attractive. The value of every node in the network is then defined precisely through its distinctiveness. In the New Game, your challenge is to make the world a better place, because of you.

---

59 | Jürgen Geuter, 'Digitale Souveränität', *connected*, 25 August 2014, https://connected.tante.cc/2014/08/25/digitale-souveraenitaet/.

LEARNING TO FLY

On February 20, 2014, the Canadian photographer Joey L. receives a Twitter message from Anthony Kurtz. He doesn't know Kurtz in person, only from Twitter. Kurtz asks whether he was in India in 2007 – seven years ago. Puzzled, Joey L. replies that yes, he had been to India: in Varanasi, a historic town on the Ganges river, frequented by pilgrims and tourists. Kurz sends a picture taken back in 2007, and asks whether that is him. The photo is a long shot of the historic buildings on the banks of the Ganges, as seen from the river. There are a lot of people in the image: boats filled with locals lining the shore, women sitting on the steps leading down to the river, people strolling along the promenade. Two of these – tiny figures in the photo – are apparently tourists. Joey asks for the high-resolution original and other photos from the set, and Kurtz sends those along as well. There, if you zoom in close enough, you can see Joey L. walking along the banks. The photo was taken on October 18, 2007. At the time, Joey was just 17 years old.

Then, on one of the images, he discovers himself taking a photograph of two women who are sitting nearby and drawing. He recovers the photo that he must have taken in that moment. His own image, in turn, shows the Ganges in the background, with all the boats from which people are taking their own pictures. One of them had to be Anthony Kurtz. Joey L. writes an ardent blog post about his experience, and is delighted at how the internet has shrunk his world: 'I Was Hidden on this Guy's Hard Drive for Over 6 Years'.[60] There are many ways to respond to *Kontrollverlust*.

In the future, these kinds of stories shouldn't surprise us much. The world has become transparent unto itself, simultaneously visible from all angles. Is it any wonder, then, that two photographers take a photo of one another taking a photo, and find each other over the internet? You can tell this story as a lurid horror tale, or as a display of collective mutual awareness.

Before air travel was invented, no one had probably ever imagined that we would some day climb into tin cans that would take off into the sky. Sitting in a chair, thousands of feet up in the air – what a loss of control! And what a gain of control! Before the airplane, traveling to India was something that was just not possible for the majority of people. This was an invention that shrank the world, and without it, a story like that of Joey L. and Anthony Kurtz never could have happened.

The New Game is an airplane, and we are already on board. It's okay to be scared, and the turbulence can be dangerous. But I think the flight is worth it. It's worth it in much the same way as boarding a plane and stepping off into a new world on the other side.

60 | Joey L., 'I Was Hidden on this Guy's Hard Drive for Over 6 Years', 15 July 2014, http://petapixel.com/2014/07/15/hidden-guys-hard-drive-6-years/.

REFERENCES

Bambauer, Jane R. 'Tragedy of the Data Commons', *Harvard Journal of Law and Technology*, Vol. 25 (2011), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1789749.

Bamford, James. 'The Most Wanted Man in the World', *Wired*, 13 August 2014, http://www.wired.com/2014/08/edward-snowden.

Beresford, Alastair R., Dorothea Kübler, and Sören Preibusch. 'Unwillingness to Pay for Privacy: A Field Experiment', SFB 649 discussion paper, no. 2011-010, https://www.econstor.eu/bitstream/10419/56724/1/654787352.pdf.

Beschizza, Rob. 'Tourists Deported from U.S. for Twitter Jokes (Updated)', *BoingBoing*, 30 January 2013, http://boingboing.net/2012/01/30/brits-deported-from-u-s-for-t.html.

Brin, David. *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?* New York: Perseus, 1998.

'Buch: Das Neue Spiel – Nach dem Kontrollverlust', *Startnext*, https://www.startnext.de/ctrlverlust/.

Burckhardt, Martin. *Digitale Renaissance: Manifest für eine neue Welt*. Berlin: Metrolit, 2014.

Claus, Robert. 'Maskulismus: Antifeminismus zwischen vermeintlicher Salonfähigkeit und unverhohlenem Frauenhass', July 2014, http://library.fes.de/pdf-files/dialog/10861.pdf.

Detel, Hanne and Bernhard Pörksen. *Der entfesselte Skandal. Das Ende der Kontrolle im digitalen Zeitalter,* Cologne: Herbert von Halem, 2012.

Detel, Hanne and Bernhard Pörksen. *The Unleashed Scandal: The End of Control in the Digital Age*, Exeter: Imprint Academic, 2014.

'Duty Calls', *xkcd*, http://xkcd.com/386/.

'E-Mail made in Germany'. https://www.e-mail-made-in-germany.de/.

Ferguson Police Department. 'Racial Profiling Data/2013', http://ago.mo.gov/VehicleStops/2013/reports/161.pdf.

Fryer, Roland G. and Steven D. Levitt. 'Understanding the Black-White Test Score Gap in the First Two Years of School'. *Review of Economics and Statistics*, Vol. 86.2 (2004): 447-464.

Fryer, Roland G. and Steven D. Levitt. 'Testing for Racial Differences in the Mental Ability of Young Children'. *National Bureau of Economic Research*, Working Paper No. 12066, 2006.

Gannes, Liz. 'SXSW: Shirky's New Opportunities in Public Sharing', *Gigaom*, 14 March 2010, http://gigaom.com/2010/03/14/sxsw-shirkys-new-opportunities-in-public-sharing/.

Geuter, Jürgen. 'Digitale Souveränität', *connected*, 25 August 2014, https://connected.tante.cc/2014/08/25/digitale-souveraenitaet/.

Gruhnwald, Sylke and Alice Kohli. 'Die Toten vor Europas Toren', *Neue Zürcher Zeitung*, 2 April 2014, http://www.nzz.ch/aktuell/startseite/die-toten-vor-europas-tueren-1.18272891.

Hank, Maike. 'Normal ist das nicht!', *Kleinerdrei*, 24 January 2013, http://kleinerdrei.org/2013/01/normal-ist-das-nicht/.

Heidenreich, Stefan. 'Datendichte und digitale Geschichte', *Docupedia – Zeitgeschichte*, 11 February 2010, http://docupedia.de/zg/Blog:%22Datendichte_und_digitale_Geschichte%22_-_Vortrag_von_Stefan_Heidenreich_zur_Projektpr%C3%A4sentation_am_11.02.2010_2010/03/05.

Heller, Christian. *Post-Privacy: Prima leben ohne Privatsphäre,* Munich: C.H. Beck, 2011.

Heller, Christian. *PlomWiki*, http://www.plomlompom.de/PlomWiki/.

Hermanin, Costanza and Angelina Atanasova. 'Making "Big Data" Work for Equality', *Open Society Foundations*, 9 September 2013, http://www.opensocietyfoundations.org/voices/making-big-data-work-equality-0.

Himmelreich, Laura. 'Der Herrenwitz', *Stern*, 1 February 2013, http://mobil.stern.de/politik/deutschland/stern-portraet-ueber-rainer-bruederle-der-herrenwitz-1964668.html.

Hirschman, Albert O. *Exit, Voice, and Loyalty: Responses to Decline in Firms, Organizations, and States*, Cambridge, MA: Harvard University Press, 1970.

iRights (Digital Copyright Information Platform). http://irights.info/.

Jarvis, Jeff. *Public Parts: How Sharing in the Digital Age Improves the Way We Work and Live,* New York: Simon & Schuster, 2011.

L., Joey. 'I Was Hidden on this Guy's Hard Drive for Over 6 Years', 15 July 2014, http://petapixel.com/2014/07/15/hidden-guys-hard-drive-6-years/.

Levinas, Emmanuel. *Totalité et Infini: essai sur l'extériorité,* Den Haag: Martinus Nijhoff, 1961.

Meiritz, Annett. 'Debatte: Man liest ja so einiges über Sie', *Der Spiegel*, 14 January 2013, http://www.spiegel.de/spiegel/annett-meiritz-ueber-die-frauenfeindlichkeit-in-der-piratenpartei-a-877558.html.

Masing, Johannes. 'RiBVerfG Masing: Vorläufige Einschätzung der "Google-Entscheidung" des EuGH', *iRights*, 14 August 2014, http://irights.info/artikel/ribverfg-masing-vorlaeufige-einschaetzung-der-google-entscheidung-des-eugh/23838.

'On Facebook, People Own and Control Their Information', 16 February 2009, *Facebook*, https://www.facebook.com/notes/facebook/on-facebook-people-own-and-control-their-information/54434097130.

OpenDataCity. 'Verräterisches Handy', https://opendatacity.de/project/verraeterisches-handy/.

OpenDataCity. 'Geheimer Krieg', https://opendatacity.de/project/geheimer-krieg-2/.

Pariser, Eli. *The Filter Bubble: What the Internet Is Hiding from You,* New York: Penguin Press, 2011.

Petzinger, Thomas. *Hard Landing*, New York: Random House, 1995.

Reißmann, Ole. 'Überwachung: BND soll weitgehenden Zugriff auf Internetverkehr in Deutschland haben', *Spiegel Online*, 13 November 2013, http://www.spiegel.de/netzwelt/netzpolitik/bnd-soll-sich-zugriff-auf-internetverkehr-verschafft-haben-a-933333.html.

Roth, Evan. http://www.evan-roth.com/about.

Schrupp, Antje. 'Über das Müssen', *Bzw-weiterdenken*, 13 August 2008, http://www.bzw-weiterdenken.de/2008/08/uber-das-mussen.

Sethe, Paul. 'Stimmen verstummt'. *Der Spiegel*, 40/1967, 25 September 1967, http://www.spiegel.de/spiegel/print/d-46353351.html.

Smiers, Joost and Marieke van Schijndel. *No Copyright: Vom Machtkampf der Kulturkonzerne um das Urheberrecht. Eine Streitschrift,* Cologne: Alexander, 2012.

Snowden, Edward. 'NSA Whistleblower Answers Reader Questions', *The Guardian*, 17 June 2013, http://www.theguardian.com/world/2013/jun/17/edward-snowden-nsa-files-whistleblower.

Taleb, Nassim Nicholas. *The Black Swan: The Impact of the Highly Improbable,* New York: Random House, 2007.

Taleb, Nassim Nicholas. *Antifragile: Things That Gain from Disorder,* New York: Random House, 2012.

Tante, Ryan. 'Apple Hides How White It Is', *Gawker*, 9 November 2011, http://gawker.com/5858020/apple-hides-how-white-it-is.

'Tell-All Telephone'. *Zeit Online*, March 2011, http://www.zeit.de/datenschutz/malte-spitz-data-retention.

Trojanow, Ilija. 'Willkür und Freiheit', *FAZ*, 1 October 2013, http://www.faz.net/aktuell/feuilleton/buecher/autoren/einreiseverbot-fuer-ilija-trojanow-willkuer-und-freiheit-12599490.html.

Tufekci, Zeynep. 'What Happens to #Ferguson Affects Ferguson: Net Neutrality, Algorithmic Filtering and Ferguson', *Medium*, 14 August 2014, https://medium.com/message/ferguson-is-also-a-net-neutrality-issue-6d2f3db51eb0.

Vingiano, Alison. 'This Is How A Woman's Offensive Tweet Became The World's Top Story', *Buzzfeed*, 22 December 2013, http://www.buzzfeed.com/alisonvingiano/this-is-how-a-womans-offensive-tweet-became-the-worlds-top-s.

Von Horst, Nicole. 'Archäologie von zwei Tagen. Was Brüderle (nicht) mit #aufschrei zu tun hat', *Word Up!*, 24 January 2014, http://literatier.wordpress.com/2014/01/24/archaologie-von-zwei-tagen-was-bruderle-nicht-mit-aufschrei-zu-tun-hat/.

Wegemann, Nikolaus. *Bücherlabyrinthe: Suchen und Finden im alexandrinischen Zeitalter*. Cologne: Böhler, 2000.

Weiler, Lars. '#aufschrei', August 2013, http://aufschrei.konvergenzfehler.de/timeline/.

Wikipedia contributors, 'Leistungsschutzrecht', 4 March 2013, http://en.wikipedia.org/wiki/Leistungsschutzrecht, accessed 16 January 2015.

WTFPDL (Modified WTFPL for the Digital Sphere). http://wtfpdl.net/.

WTFPL (Original 'Do what the fuck you want to Public License'). http://www.wtfpl.net/.

Wu, Tim. 'Network Neutrality, Broadband Discrimination', *Journal of Telecommunications and High Technology Law*, Vol. 2 (2003) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=388863.

FOR MORE INFORMATION SEE
networkcultures.org/
publications

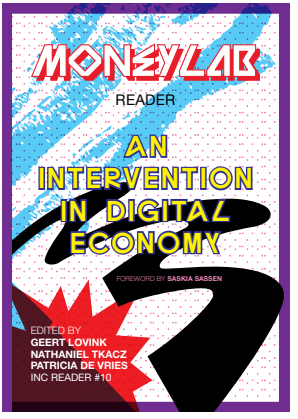
INC PUBLICATIONS

INC publication series include essay collections, commissioned writings on the intersection of research, art, and activism, and theoretical works with an international scope. Experiments are done with multiple formats such as print, EPUB, and PDF, keeping quality standards in content and design high at all times.

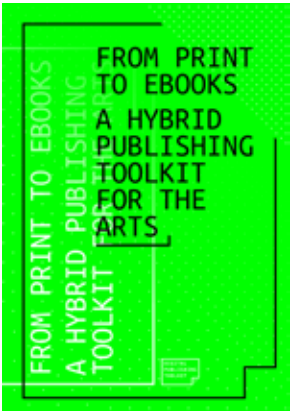
Download the EPUB edition of Digital Tailspin: Ten Rules for the Internet After Snowden directly from bit.ly/DigitalTailspinEpub

Brooke Wendt, The Allure of the Selfie. Download the EPUB directly from bit.ly/AllureSelfieEpub

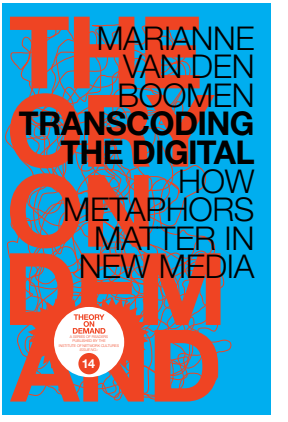
Henry Warwick, Radical Tactics of the Offline Library. Download the EPUB directly from bit.ly/radicalepub



INC Reader #10: Geert Lovink, Nathaniel Tkacz, and Patricia de Vries (eds), **MoneyLab: An Intervention in Digital Economy**, 2015.



From Print to Ebooks: A Hybrid Publishing Toolkit for the Arts, 2015.



Theory on Demand #14: Marianne van den Boomen, **Transcoding the Digital: How Metaphors Matter in New Media**, 2014.

Privacy, copyright, classified documents and state secrets, but also spontaneous network phenomena like flash mobs and hashtag revolutions, reveal one thing – we lost control over the digital world. We experience a digital tailspin, or as Michael Seemann calls it in this essay: a loss of control or *Kontrollverlust*. Data we never knew existed is finding paths that were not intended and reveals information that we would never have thought of on our own.

Traditional institutions and concepts of freedom are threatened by this digital tailspin. But that doesn't mean we are lost. A new game emerges, where a different set of rules applies. To take part, we need to embrace a new way of thinking and a radical new ethics – we need to search for freedom in completely different places. While the Old Game depended upon top-down hierarchies and a trust in the protective power of state justice systems, the New Game asks you to let go of all these certainties. Strategies to play the game of digital tailspin rely on flexibility, openness, transparency and what is dubbed 'antifragility'. In *Digital Tailspin: Ten Rules for the Internet After Snowden* Michael Seemann examines which strategies are most appropriate in the New Game and why.

Michael Seemann studied Applied Cultural Studies in Lüneburg. Since 2005 he is active on the internet with various projects. He founded twitkrit.de and Twitterlesung.de ('reading Twitter'), organized various events and runs the popular podcast wir.muessenreden.de. In 2010 he began the blog CTRL-verlust, about the loss of control over data on the internet. In 2014 he published *Das neue Spiel* after a successful crowdfunding campaign. Now he blogs at mspr0.de and writes for various media like Rolling Stone, TIME online, SPEX, Spiegel Online, c't and the DU magazine. He gives lectures on whistleblowing, privacy, copyright, internet culture and the crisis of institutions in times of *Kontrollverlust*.

Amsterdam, The Netherlands 2015
ISBN 978-90-822345-8-9

institute of network cultures
Amsterdam University of Applied Sciences
AMSTERDAM CREATIVE INDUSTRIES NETWORK
STICHTING DEMOCRATIE EN MEDIA