DATA LOVE

THE SEDUCTION AND BETRAYAL OF DIGITAL TECHNOLOGIES

ROBERTO SIMANOWSKI

Columbia University Press *New York*

Columbia University Press
Publishers Since 1893
New York Chichester, West Sussex
cup.columbia.edu

Library of Congress Cataloging-in-Publication Data
{to come}

Columbia University Press books are printed on permanent
and durable acid-free paper.
This book is printed on paper with recycled content.
Printed in the United States of America

c 10 9 8 7 6 5 4 3 2 1

COVER IMAGE:
COVER DESIGN: *Designer Name*

References to websites (URLs) were accurate at the time of writing.
Neither the author nor Columbia University Press is responsible
for URLs that may have expired or changed since
the manuscript was prepared.

For Luciana
Whom I love more than any data

Lots of knowledge fits into a hollow head.

—Karl Kraus, *Dicta and Contradicta* (1909)

And youth is cruel, and has no remorse
And smiles at situations which it cannot see.

—T. S. Eliot, "Portrait of a Lady" (1920)

He was found by the Bureau of Statistics to be
One against whom there was no official complaint,
And all the reports on his conduct agree
That, in the modern sense of an old-fashioned word, he was a saint.

—W. H. Auden, "The Unknown Citizen" (1939)

CONTENTS

PART III: THE JOY OF NUMBERS

PART IV: RESISTANCES

PREFACE

Praised be the technology that allows us to listen to Berlin's "Info Radio" in the Swiss Alps or in a Hong Kong subway! Praised be the city map that describes itself when clicked on and—without our having to study it—leads us to the place we seek! Praise also to Shazam and all the apps that identify an unknown song, directly linking us to both the lyrics and the video! Praise to the online travel plan, showing all our connections within seconds and selling us the ticket as well! And likewise praised be the asthma inhaler that uses GPS to warn other patient-users away from those areas that they should avoid!

We love information. We always have. We used to gather around early wanderers to hear tales of faraway places when it was rare to find books outside of monasteries. We invented the telegraph because we grew impatient waiting for travelers. We waited as eagerly for the morning paper as for the evening news on radio or on TV, as if they were only ever presenting good news. Now we get the latest news by the minute, and we even treat our own lives as news, updating ourselves around the clock via Facebook, Twitter, or Instagram. Our eagerness to share information matches our greed for taking it in.

We view every mountain and every lake that has not yet been surveyed as an insult to human reason. When we communicate, watch videos, jog, eat, or sleep, a limitless fervor drives us to access the networks of ourselves and our social life. We are on a mission to produce data ceaselessly and in perpetuity. Every tweet is regarded as a contribution to knowledge. We believe in progress through analysis, which will make our lives easier and more secure.

We love ourselves in the form of the blue arrow on Google's map, and we eagerly anticipate the advent of the smart city where all citizens' movements are tracked, creating instant taxi stands wherever they happen to be needed. We're looking forward to the "wearable computers" that will permit us to remain online without taking our hands off the steering wheel. We thank Google for reminding us where we are, what we should know, and what we will want to do next.

An information society is one in which all information is just seconds away, information about everything, everywhere, and at all times: "information at your fingertips." We live in an information society. And we love it!

In 2011 the title of a Berlin conference called Data Love was justified in the following way:

> Today, data is what electricity has been for the industrial age. Business developers, marketing experts and agency managers are faced with the challenge to create new applications out of the ever-growing data stream with added value for the consumer. In our data-driven economy, the consumer is in the focus point of consideration. Because his behaviour determines who wins, what lasts and what will be sold. Data is the crucial driver to develop relevant products and services for the consumer.[1]

This emphatic promotion is affirmed by the classic business adage: "What can't be measured can't be managed." Both statements show that data love is in no way unconditional. It is devoted to data as information that gives a meaningful form to measurable facts.[2]

To be sure, "data love" is a euphemism. It is the palatable alternative to the central concept of digital-information society: big-data mining—the computerized analysis of large collections of data intended to reveal regularities and previously unknown correlations. “Love” refers to both aspects of the dual nature of the mining: Corporations love big data because it allows them to develop customized products, and consumers love big data for the same reason. This, at least, is what the quotation proposes to us: Mining data leads to added value for customers. Data love is a phenomenon not only of the society of control but also of the consumer society. And data love thrives on precisely the same data that security and privacy would claim to protect.

At the same time, data love is embraced by Internet activists who advocate free communication and proclaim as “principles of datalove” that data must flow, must be used, is neither good nor bad nor illegal, cannot be owned, is free. This notion opposes “the misconceptions of politicians, who keep trying to establish exceptions for the expression of certain types of data”—such as “hate speech” or “child porn”—and postulates an unconditional love of data regardless of that data’s nature or possible misuse: “Datalove is so exciting! It’s all about the availability of data. What people do with it is not the question. The point is: people need data. Need to get it. Need to give it. Need to share it. Need to do things with it, by means of it.” This is another and different form of data love, conceptualized as a desire to know or even as a second wave of Enlightenment: “Datalove is about appreciation of being able to understand, perceive and process data altogether for the enjoyment and progress of all sentient beings.” Business entrepreneurs and marketing experts can easily subscribe to this call for free data flow. What is missing in this enthusiastic embrace of data is a sensitivity to the potential for conflict between data mining and privacy. Claiming that “if some data is meant to be private, it should not reach the Internet in the first place” sounds an awful lot like the rhetorically effective “nothing-to-hide” argument one generally hears from intelligence agencies and big software companies.[3]

This book describes the promises and dangers of data’s ambivalent love. It discusses the changes affecting the human situation and considers data love not as the obsessive behavior of overzealous intelligence agencies, clever businessmen, and Internet (h)ac(k)tivists but rather as the entanglement of all those who—whether out of stinginess, convenience, ignorance, narcissism, or passion—contribute to the amassing of ever-more data about their lives, eventually leading to the statistical evaluation and profiling of their individual selves.

Those who discuss the NSA scandal of the summer of 2013 only as a matter of the tension between the two basic rights to freedom and security are failing to see the more problematic or even aporetic aspect of the issue. The imperative of transparency implemented by social online portals, self-tracking applications, and the promises of the Internet renders data gathering an everyday phenomenon. What is technologically feasible becomes all but universally irresistible. Naturally, this is especially true when it comes to intelligence agencies. But the same circumstances hold for the consumer economy and for those in charge of infrastructural government, that is, traffic control, urban planning, public-health administration, etc. The majority of people are looking forward to all the promises of data mining. Herein lies the philosophical problem that goes beyond the political discussion of the NSA scandal. Data love leads to a double-edged potentiality: the reconciliation of society with its security apparatus. In the age of increasing digitization of human communication, the logical consequence for everyone is the so-called full take of all data on everyone and everything. Against our wishes and our declarations to the contrary, privacy in the twenty-first century becomes outdated.

The effects of this unrestrained exploitation of personal data have been compared with ecological disaster. It is maintained that just as the individual use of energy is not a merely personal matter, so dealing with personal data has social consequences with ethical implications. A discussion from this perspective goes beyond the easy citizen-versus-state logic. However, simultaneously, it undermines our thinking through the problem in a new way. For while the ecological movement's ethics are focused on the preservation of human existence—which no one would oppose—the concept of "data disaster" basically operates in relation to a culturally conservative position for which privacy is a value that should remain untouched. This idea of privacy as an inalienable right is compromised by the willingness——not only of the younger generation—to give up personal data and, inadvertently, by all those who blindly agree to insidious terms of service. If, in the context of the NSA scandal, people have talked about a "cold civil war," then this should be understood as a conflict *within* every citizen—namely, between an interest in data mining's advantages and a fear of its disadvantages.

The principal agencies of big-data mining are the number crunchers and the data scientists whose current job descriptions increase in sex appeal and promise remuneration in the millions. Unnoticed and inexorably, their contributions to increasingly efficient methods of data management and analysis are changing cultural values and social norms. Software developers are the new utopians, and their only program for the world is programmability, occasionally garnished with vague expressions of the emancipatory value of participation and transparency. The secret heroes of this "silent revolution" are the algorithms that are taking over humanity. On the one hand, they increasingly assume "if-then" directives, enforcing them immediately and relentlessly. On the other hand, they reveal more and more if-then correlations and, armed with this new knowledge, pressure society to intervene on the *if* level in cases of unwelcome *then* effects.

The actual objects of fear are not NSA or Big Brother but *predictive analytics* and *algorithmic regulation*. They are kindred spirits of the *technocratic rationality* that was once discussed critically as the dark side of the Enlightenment under the headings of "reification" and "lack of responsibility." In the wake of big-data mining the dangers of technocratic rationality reveal themselves imminently as promoting an increasingly statistical view of society. We need a discussion that goes far beyond concerns over restoring the security of e-mail communication—as the chief replacement for a legally and physically inviolable postal system—in the face of digitization and global terrorism. The larger question pertains to the image modern society has of itself and how willing society is to allow its data scientists and their technologies to reshape it.

Daily journalism aside, discussions show that developments in the philosophy of science also support the paradigm of data mining in parallel to these problems of surveillance and privacy. With statistically determinable knowledge in clear view, the "end of theory" has been declared, and even the humanities strive to become "hard" science by generating quantitatively attested "knowledge." This shift from the subjective, from the ambivalence of interpretation, toward algorithmic methods of analysis, fulfills itself in a vision of "semantic publishing," formalizing statements into units that can be isolated autonomously, like entries in a database. From cultural studies' point of view, we see just how far away we have moved from Humboldt's educational ideals and from Lessing's conception of knowledge, one that discovered the purpose of mankind not so much in finding and managing the truth as in the process of searching for it.

The question worrying many of those who are concerned with the cultural effects of the present technological development is this: What possibilities does the individual have to intervene in this process? The answer must begin with the recognition that we do not speak for the majority. As long, for example, as Google is able to present itself as the eyes of God in the sense of caring rather than overseeing and judging, then any protest against big-data mining will raise objections from all those people who benefit from Google's "care." The debate on surveillance and privacy, instigated by the NSA scandal, ignores this general complicity and agreement. We do want Google to know everything about us so that it can fulfill its customer care as effectively as possible—from personalized search results via geolocal recommendations to suggestions as to what we should do next. We agree that the *smart things* in the Internet can only make our tasks easier to the extent to which they—and thus all who have access to their data—know about us.

Disciplining the various intelligence agencies is the only common denominator upon which society can still partway agree. And not even in this case is everyone of one mind. One needs to ask why people as citizens insist on a private sphere that they blithely ignore as consumers. In this context, those who call for the rescue of the Internet insofar as it is abused as a means of surveillance rightfully remind us of the hopes that were once associated with this new medium as a locus of emancipation and democratization. They also echo the intellectuals, today derided or forgotten, who back in the 1960s and 1970s called for the improvement of society, admonishing the disinterested people: There is no right life in the midst of a wrong one.

Changing media is even harder than changing societies. Apart from the social realm from which they emerge, media have their own inherent agenda that they are determined to fulfill. With respect to computers and the Internet this implies calculating, connecting, regulating. Big-data mining is not a byproduct of media development; it is its logical consequence. It radicalizes the Enlightenment impulse for mapping and measuring, something that today is inevitable and unavoidable because anything that happens digitally will produce data. Data analysis—regardless of any particular regime of data protection that may be in place—is not a "car accident" on the data highway; it is the actual destination. Data love—our love for data and its love for us—is the embrace that hardly anyone in this day and age can avoid. The forms it will take, what cultural and social side effects it will produce, and the ideas and reflections one can have about it from the perspective of philosophy or cultural studies are the subject of this book.

DATA LOVE

PART I

BEYOND THE NSA DEBATE

1

INTELLIGENCE AGENCY LOGIC

In the summer of 2013 the twenty-nine-year-old IT specialist Edward Snowden flew into a foreign country carrying with him secret documents produced by his employer, the National Security Agency of the United States (NSA). From the transit zone of the Moscow airport and with the help of the *Guardian* and the *Washington Post*, he informed the world about the extent of the surveillance of telephone and Internet communications undertaken by American intelligence agencies. In doing this, the whistleblower Snowden became much more successful than Thomas Drake, a former department head at the NSA who, with the same motives, had criticized the excessive surveillance practices of the NSA first through official channels and then in 2010 by divulging information to a journalist from the *Baltimore Sun*, for which he was later accused of espionage. Snowden's disclosures triggered an international sensation lasting many months, creating what historians at the time characterized as the last great epiphany to be experienced by media society.

This is how a report on the events of the NSA scandal of 2013 might begin in some distant future. The report would evaluate the event from a respectful historical distance and without the excitement or disappointment of earlier historians. From the distant future, this moment of revelation would prove to have been the last outcry before the realization that there were no alternatives to certain unstoppable technological, political, and social developments. The report from the future would reconstruct the case with historical objectivity, beginning by explaining how world leaders reacted.

The United States declares Snowden's passport invalid and issues a warrant of arrest for the breach of secrecy and theft. The Brazilian president protests at the United Nations over spying on Brazilian citizens (including herself). She cancels her planned meeting with the president of the United States and by creating an investigative committee again proves her capacity to act after the traumatic experience of the "#vemprarua" upheavals in her own country. Ecuador—its embassy in London housing the founder of WikiLeaks, Julian Assange—offers asylum to Snowden, thereby forgoing U.S. customs benefits. Germany denies Snowden's request for asylum on the technicality that one cannot file an application from a foreign country. Russia grants asylum to Snowden for one year, provoking a further cooling of its relations with the United States and immediately causing the cancellation of a planned summit meeting between Obama and Putin.

Net theoreticians appreciated Snowden's act because it forced society to debate matters that were long overdue for discussion. But acclaim did not come only from this quarter. Peer Steinbrück, the Social Democratic Party's candidate for the chancellorship of Germany, and the European Union's commissioner of justice, Viviane Reding, thanked Snowden for his civil courage and the debate he initiated.[1] Even a former president of the United States, Jimmy Carter, supported Snowden. The state's invasion of the private sphere, he claimed, had been excessive, and Snowden's disclosure would in all likelihood prove useful in the long run.[2] The current president remained inflexible in his thinking, although at a White House press conference on August 11, 2013, he conceded that the work of the NSA had to be more transparent. He announced that a commissioner for data protection would be appointed. But President Obama was vehemently opposed to the idea that Snowden should be treated as a patriot and not as a traitor: "No, I don't think Mr. Snowden was a patriot. I called for a thorough review of our surveillance operations before Mr. Snowden made these leaks. My preference, and I think the American people's preference, would have been for a lawful, orderly examination of these laws." Even if it were the case that Obama was a step ahead of Snowden, there's no denying that Snowden's act accorded with the impetus of Obama's review. Nonetheless, Snowden's nomination for the Nobel Peace Prize in 2014 underlines how different the reactions to Snowden's "treason" have been, especially when it comes to assessing the effect of his act on the world order.

The disclosures and accusations did not implicate the NSA alone. The British intelligence agency was also involved, and, as was later discovered, the German Federal Intelligence Service was working closely with the NSA, which should not have surprised anyone since, after all, a part of the September 11, 2001, team of assassins had come from Hamburg. It was generally known and widely accepted that this catastrophic event had justified many governmental data breaches and restrictions of civil liberties in the new millennium. The belief that defense against international terrorism inevitably requires limits on data protection was shared by the Obama administration and many other politicians. Even moral philosophers agreed. Peter Singer, for example, valued the gain in security over the loss of privacy in his essay "The Visible Man: Ethics in a World Without Secrets" (2011) since he considered privacy a recent, chiefly Western phenomenon in the history of mankind, one whose importance he relativized. It was particularly easy at the time, our future report might conclude, to smooth the way for the transition from a democratic society to a surveillance state by way of fear and "prudence."

If the future report were written by a German, it might at this point possibly refer to Christian Heller, who, simultaneously with Singer but independently, had published a sort of guide to the inevitable in his 2011 book *Post-Privacy. Prima leben ohne Privatsphäre* (Post-privacy. How to live well without a private sphere). Heller, the future report may then state, overcame the historical trauma of surveillance that has haunted German collective memory since the Third Reich and then the German Democratic Republic. It is possible that the report would regard Heller's book as igniting the spark for "the transparent 90 percent," the late 2010s citizen's movement that demanded more intensive security controls and attracted more and more followers. With their slogan "we have nothing to hide," they refused to risk their own lives for a minority's excessive adherence to privacy. The report would show how the followers of this movement proudly repudiated any kind of encryption in their digital communications, how they voluntarily installed the federal government's Trojan software on their computers and mobile devices, and how they were rewarded in return with VIP biometric security passes that granted them the use of special airplanes, subways, and buses.

No matter how these reports from the future would conclude, such a civil movement could be counted on to subscribe to statements such as the one from the German secretary of the interior at the time, Hans-Peter Friedrich of the Christian Social Union, who maintained that security is a "superfundamental right," or like the one by the former secretary of the interior, Otto Schily, the "red sheriff" of the Social Democratic Party, who declared that law and order are social-democratic values and that the biggest danger does not come from the state and its intelligence agencies but from terrorism and organized crime.[3]

Secretaries of the interior are, by nature, partisans of the work of their intelligence agencies, over and above party-political lines. After all, the government issued the mandates for which these agencies are now being publicly scolded, namely, to ward off threats to the inner security of their countries by way of the undercover investigations of possible risks. As Friedrich said in the context of the NSA affair, nobody should be astonished or upset when intelligence agencies use the latest cutting-edge technologies. Intelligence agencies want to secure and enhance their effectiveness just as much as any other functional social system; whatever is technologically possible will be used. For this reason, ever since 9/11 intelligence agencies had been dreaming of the "full take" of all data from all citizens. What had failed to materialize until then, because of financial and technological shortcomings, became a real option with the increasing digitization of society. The consensus was that those who did not use the new possibilities for data collection and evaluation were refusing to work properly, which in this realm of work might almost be regarded as treason.

It is obvious that the situation after 9/11 cannot be compared with that under the Stasi in former German Democratic Republic. In the Federal Republic of Germany the intelligence agency is constitutionally legitimized and controlled by parliament, even if not all members of parliament see it this way and continue to demand more transparency. The stronger argument is a technical one: Surveillance is no longer done by an intelligence agent who scrutinizes the letters and conversations of an individual but by software that searches for certain key terms. Even though the surveillance is more all-encompassing because of its use of modern technologies, it is also more anonymous and more democratic because it is not aimed at specific individuals but at all of society, including the intelligence agent himself. One could regard this as the perfect solution to an internal contradiction within every democracy: As the work of intelligence agencies becomes more and more effective and cost efficient, the private sphere of citizens is increasingly protected by the machinery of such "distant reading."

2

DOUBLE INDIFFERENCE

THE snooping around by the NSA and the support it received from other intelligence agencies was not the most scandalous aspect of the NSA affair. The real scandal lay in the helplessness of politics and the disinterest it revealed. The German president, who, as the former head of the Federal Commission on Stasi Affairs, should have been particularly sensitized regarding this subject, did not speak up at all. The chancellor spoke of the Internet as a "new territory for us all" and assured the public that on German soil German law has to prevail, as if the Internet could be bound to national laws by way of an increased insistence from the executive powers. The Social Democrats demanded complete clarification, as if they had nothing to do with setting the course for effective collaboration with the NSA and for a law on data retention during their own time in government. Others urged citizens to secure their own data more responsibly, as if it concerned only data presented voluntarily on Facebook and Twitter, as if all was well again as soon as cookies were blocked, e-mails encrypted, and the browser archive deleted every evening. Hardly any apps are at the disposal of those who are worried about their data since terms of use are not up for negotiation; apps triumphantly appear in the hard core of "take it or leave it." Protecting one's own data in this case means forgoing the use of a multitude of helpful, interesting, and simply entertaining programs. Perhaps there are a few everyday heroes who stubbornly refuse to click on “accept” if they feel that the appetite of an app for user and usage data is too great, but those who do this consistently must then ask themselves why they even own a smart phone if they use it only to make phone calls.

Nevertheless, at the time, the ignorance of the bulk of the population was scandalous. Even though a few folks demonstrated against the intelligence agencies’ surveillance, the reaction did not measure up to the seriousness of the incident, which some even labeled a “digital Fukushima.”[1] Most of those who were against surveillance still didn’t do anything against it, saying that they had nothing to hide anyway. This gesture of appeasement is not only naive; it is also immoral, as can be seen from a concurrent newscast reporting on the marriage of two men in a Protestant church. Still forbidden by law and frowned upon several decades ago, this was now accepted by society and even consecrated by the church. In other words, from today’s perspective, many people who had something to hide in the past—including those from the less recent past, such as doctors illegally dissecting corpses—had never been bad to begin with.

Those who advocate transparency across the board risk allying themselves with prevailing moral norms against the claims of minorities—or of new scientific findings, for that matter. In a democratic society that is aware of the partially backward-looking nature of its written and unwritten laws, it should be the duty of all citizens—a “superfundamental duty”—to protect the right to anonymity by practicing it themselves. This is the only way to cancel out the prospect that in the future everyone will be under suspicion if they attempt to evade outside control of their behavior—even if only by turning off their GPS. Considering that the laws of a democracy can never be either state of the art or carved in stone, this deserves serious reflection. Germany’s history presents a frightening example. At a certain time in the past German citizens treated their data openly and did not conceal their Jewish ancestry, having no idea that this would lead to their deaths. How are we to know today which part of our “harmless” data will at some point be turned against us under future power structures?

In the present circumstances the statement “I have nothing to hide” is naive. Even if we don’t care whether our GPS data will divulge with whom and where we have spent the night, we should not assume that others cannot figure us out better than we can ourselves. People are more than the sum of their data. Hidden insights are discovered in the digital summary and in comparisons, in the insights gained from statistics, and in the recognition of behavioral patterns. A famous, often-quoted example is that of the father from Minneapolis who complained to the retailer Target over the ads for baby products being sent to his underage daughter. Target had assumed her to be pregnant because the purchasing behavior of this woman had corresponded to the statistically generated consumption patterns of pregnant women. As it turned out, Target actually did know more about its customer than the father did about his daughter. What seems harmless to the initiator of an informationally implicated transaction—ordering a book from Amazon, commenting on YouTube, searching for certain terms through Google, or just buying certain articles—is a piece in the puzzle of a complex profile for big-data analysts, a profile that can tell them more about us than we know or want to know about ourselves. The algorithm is the psychoanalyst of the twenty-first century, delineating patterns of behavior that had previously remained hidden. The sales pitch for the Nike+ iPod Sport kit with pedometer is formulated precisely along these lines: “See all your activity in rich graphs and charts. Spot trends, get insights and discover things about yourself you never knew before.”[2] How is it possible to exercise our basic rights to informational self-determination when the analyst brings things to light of which we weren’t ourselves aware, all without asking us whether we permit the use of this information somewhere else or not?

No matter how one might assess or evaluate sensitivity to the breach of privacy in the population, suggestions for averting such breaches not only cited national and European laws against the media colonization of the United States but also made use of European technologies.[3] One response was an initiative by the German instant-messenger provider Whistle.im that promised—

in contrast and in response to the data-hungry WhatsApp—end-to-end encryption along with an allusion to German workmanship: "Secure Instant Messaging. Made in Germany" was their slogan. National regulation as a selling point for marketing on the Internet—what a change vis-à-vis the former animosity against state institutions! And how self-confidently and unceremoniously Perry Barlow's *Declaration of the Independence of Cyberspace* (1996) stated it at the time: "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone." Whereas now we were hoping for help from the good old nation-state against the corporations of Silicon Valley.

Of course the subject was not a new one. For a long time the Internet has been discussed as a form of neocolonialism because by way of the Internet Western technophilia and its forms of communication have come into their own worldwide. And so the tedium of "downtime," which had hardly existed before and outside of the "carpe diem" dogma, becomes a lifestyle disease everywhere else because of our permanent communication over mobile media. Communities that in traditionalist cultures had the authority to determine the individual's life are all of a sudden confronted with flexible concepts of friendship in social networks.[4] In the context of the NSA debate, the media's neocolonialism is now also internal to the Western world, for example, as structuring conflicts between German culture and American technologies. But the lines of conflict are only seemingly aligned with national values; it is mainly the "digital immigrants" for whom German technologies with German data-protection laws are precious. The majority of the digital "natives" will continue using WhatsApp and will possibly do so more than ever since the transparency-apostle and data-octopus Facebook bought the company at the beginning of 2014 for nineteen billion dollars. What is treated as colonization is in fact fundamentally a generational conflict.

It is no surprise that despite this "intranational" tension the public debate remained focused on its international dimensions, chiefly discussing the extent to which the NSA was investigating the data of German citizens on German soil. Nation-states are better able to position themselves against another nation-state than against a technology operating globally and virally. When new disclosures and more memorable images—like the mobile phone of the German chancellor or the American "center of espionage" in the heart of Germany's capital—brought the NSA debate back onto the political agenda and eventually led to a special meeting of parliament, the discussion limited itself to the problem of Germany's sovereignty vis-à-vis the United States. This certainly is an important subject—just as important as the question of parliamentary control of the intelligence agencies and the propriety of its procedures. However, the essential debate—the radical digitization of society, practiced daily by increasing cohorts of chiefly digital natives—was thereby evaded.

3

SELF-TRACKING AND SMART THINGS

WHEN the net critic Evgeny Morozov calls the American spies "dataholics" in a commentary on the NSA affair, demanding that they be committed to a "big data rehab" clinic, this represents a merely rhetorical gambit that he himself relativizes in the course of his article.[1] Morozov knows all too well that Russia, Snowden's sanctuary, loves, in this instance, the traitor more than the betrayal. After all, the criticism leveled against the NSA applies equally to the Russian intelligence agency, a fact that Morozov himself has addressed in the chapter "Why the KGB Wants You to Join Facebook," from his 2011 book *The Net Delusion: The Dark Side of Internet Freedom*. Yet it is not only the intelligence agencies that are addicted to limitless data love. Their coveting of "complete capture" finds its parallel—and here precisely lies the paradox of a possible reconciliation between society and its intelligence agencies—within society itself not only in the form of the widespread endorsement of smart things but also in what has come to be known as the self-tracking movement.

Commonly also referred to as the "quantified self," the culture of self-tracking has been developing for years, generating products like Fitbit, Digfit, Jawbone's Wristband, and Nike+, which monitor—and thereby control—the frequency of steps and pulse and thus also how we move, sleep, and eat. The imperative of absolute transparency is changing its character, promising that control will lead to self-awareness. Initially, it is striking to what extent the discourse of self-tracking is self-deluding in its populist form. The slogan connecting self-observation and self-optimization is "If you can measure it, you can learn to improve it."[2] Another slogan admits to the connection between technology and control ("If you can measure it, someone will . . .") but suggests that being proactive (". . . and that someone should be you") offers reassurance and benefit.[3] Of course one does not keep one's sovereignty over personal data by measuring oneself and by feeding the results into the system on the server of the provider. Instead, the statement underlines what Zygmunt Bauman has described as a "second managerial revolution" in claiming that the observation of man is taken over by the individual him- or herself, discipline replaced by self-discipline.[4] It is equally misleading when self-trackers cast themselves as in the "Know Thyself" tradition of the Oracle of Delphi,[5] which regarded self-knowledge as the recognition of one's own imperfections and limitations and which categorically did not mean an optimized "living by numbers."

Beyond the immediate goals of self-optimizing, self-tracking could be described as unconditional data love. Like any true love it promises no financial gain, nor does it have a reasonable goal. What a young self-tracker "who tracks everything from his mercury levels to his vitamin D consumption" announced in 2008 also holds true for others today, and even more so: "There's so much info that it'd be a shame not to track it."[6] To stay with the metaphor, true love surmounts the conventions of rationality and burns for the answers to far-fetched questions, like whether one falls asleep more quickly when standing on both legs for several minutes beforehand or how often one is typing each letter of the alphabet on one's keyboard.[7]

Nevertheless, the notion that self-trackers love data more than they love themselves would be presumptuous. The "unconditional" love for data of any kind is characterized by aspiration for a subsequent rationalization when new scientific methods create important insights from seemingly useless data about the producers of this data and thus society itself. This "unconditional" love, this aspiration for scientific insights, indicates that the undeniable obsession of self-trackers is not pure narcissism. Their data fetishism contains a social component that is initially expressed by making their personal data public and in helping others—fellow citizens, sociologists, physicians, traffic planners, and so on—understand people and society better.[8] From this perspective self-trackers are the avant-garde of an extraacademic self-study. They produce contextual, problem-oriented knowledge beyond the existing hierarchies of knowledge creation, thereby modifying the relationship between the sciences and society and echoing the statements of sociologists of knowledge since the beginning of the century. While in the course of modernity it has always been science that has spoken to society, now society "responds" to science in the guise of "lay experts."[9]

Smart things and the Internet of things provide another way of reconciling intelligence agencies with their citizens. This mantra was also cited by Morozov and others during the debate on data protection and privacy in the wake of the NSA scandal, but it hardly had the chance to gain ground against new disclosures, personal tragedy, and smashed hard disks. Yet the scenario of software-enabled everyday objects communicating with one another in order to reach programmatic decisions would have the potential for generating fascinating media spectacles: the swimming pool that heats up because a barbecue has been entered into the calendar, the fridge placing an order with the supermarket when the milk has reached its expiration date, the GPS that is aware of traffic jams and construction and automatically alters the car's itinerary. The Internet of smart things frees human intelligence from the menial tasks of analyzing situations with procedural consequences because the computer can do this work much faster and much more reliably. This is our liberation, freeing us to pursue higher goals, as the enthusiastic promise reads, but with, today, no clues as to where we might look for these goals.

At the same time, we are paralyzed by this very liberation. Marshall McLuhan, one of the founders of media studies, once upon a time called media "extensions of man": the elongation of arms (hammer, pistol), of legs (bicycle, car), of eyes (binoculars, microscope), and of memory (writing, photography). With the Internet of things, the computer now not only takes over calculation but also the observation and analysis of our environment (reasoning). For McLuhan, the dark side of the extension of organs was also an amputation because the advent of script does not train our memory any more than our legs develop muscles while we are driving. With the Internet of things a new amputation takes place, namely that of privacy. Not only do smart things cause our reasoning to atrophy, but they do so in the process of assimilating all possible personal data about us. If we don't feed them, they cannot serve us. The pool will remain cold when we don't allow it to see our calendar; GPS hardly helps when we don't tell it our destination. Smart things can only communicate to one another what they know about us, and if their service is based on intimate knowledge, then the breach of privacy happens for the sake of efficiency rather than control.

On this basis we will give these services—global players on the Internet—the very data that we don't want our intelligence agencies to have. As things stand, most of us find it a promise rather than a threat that Google is always attempting to improve the categorization of our situation, interests, and whereabouts so that at any time it can feed us recommendations about restaurants, shops, places of interest, and potential spouses in our vicinity. With the prospect of more efficient information management even a blatant technology of surveillance such as Google Glass may finally become socially acceptable. The problem of surveillance is not a political or economical one, although it is that as well; it is first a technological, philosophical, and anthropological one. Morozov calls it the "ideology of 'information consumerism.'"[10] This ideology—and this is the real scandal—surpassed the reach of the intelligence agencies by embracing everyone.

4

ECOLOGICAL DATA DISASTER

Future history "books" will report that the paradigm change from a culture of personal privacy to one enforcing the absolute transparency of individual life was put into effect not only under the banner of measurement but also under that of networking. One will read that in the twenty-first century, the Internet of things inaugurated the triumph of artificial intelligence, given human complacency, over the remaining attempts at data protection. It consolidated objects and activities and simplified people's lives by way of control. Its immense accumulation of data was a paradise for all those interested in human behavior on a grand scale: sociologists, advertising experts, insurance companies, physicians, traffic and urban planners, law enforcement, and other agencies of security. Although the process was occasionally troubled by data protectors, for a long time the vast majority of the population had already been cooperating with the state and commercial data collectors. The majority had permitted a glimpse into its buying behavior via the supermarket discount card, and it was now "selling" its digital communication—or, rather, just giving it away, considering the value generated by the data for others. It was doing so, in fact, not only to get free Internet service; one didn't want to do without GPS either, not even when it began to cost more. Even Google Glass was, eventually, a great success, maybe because it gave everyone a place at the heart of a personal surveillance center in which one forgot that this technology had been set up chiefly in order to survey surveillance. At some point most people had acquired an "intelligent trash container" that although it no longer worked under the banner of self-optimization or information management was nonetheless serving governmental control by registering whatever was being tossed into it and notifying the town hall as to whether recycling was being done correctly.[1]

Future historians will identify the precursors of this development and use them to justify the status quo. They will refer to the Dutchman Alex van Es, an early-adopting pioneer of self-tracking who, in 1998, had already published the contents of his trash bin on the website icepick.com using a barcode scanner, proving that no obsession with data mining can be so absurd as not to be converted instantly into a business plan. One will immediately be reminded that the idea of surveillance had already been contemplated by the avant-garde artist Fernand Léger for a film that was to record twenty-four hours in the everyday life of a man and a woman without their knowledge (1931), as well as in Dan Graham's project *Alteration of a Suburban House* (1978), which was to replace the wall of a home with glass and thus bring the life of this family onto the neighborhood stage—both ideas quite some time before Peter Weir's *The Truman Show* (1998). These predecessors demonstrate the extent to which art, commerce, and control are interconnected. Future historians will also report that users of the intelligent trash container—which became generally accepted in the 2020s—received a discount on the cost of their garbage disposal and that "the transparent 90 percent" movement filed an application to revoke the security passes for anyone in a household that refused to participate in the "Smart Bin, Safer City" program.

On the background of these cultural-historical findings one might agree with Morozov that the commercialization of data cannot be prohibited by law as long as it is driven by the wishes of the people. Thus the debate in the wake of Snowden's disclosures revolved, instead, around questions of how to prevent Internet companies and intelligence agencies from collaborating. Morozov called this the reaching for the "low-hanging fruit,"[2] a political maneuver predicated on the delusion that one could keep state institutions from accessing commercially collected data. It is difficult to believe that politicians would allow this self-disempowerment vis-à-vis the commercial realm. After all, the state's intimate knowledge of the life of its citizens guarantees a more efficient fulfillment of its duties: lowering the cost of healthcare by detecting disease patterns early and introducing preventive care in cases of clearly detrimental behaviors, fighting against tax evasion and fraudulent social-security benefits through detailed knowledge of its citizens' buying habits, improving control of traffic flow by analyzing patterns of mobility, allowing for better city planning through a more accurate knowledge of spatial use, more efficiently managing energy by analyzing consumption profiles, and optimizing educational policy by gathering insight into individual patterns of interest and behavior.

No state will have any objection to knowing more about its citizens. On the contrary, every state will want to put at its disposal the data generated both through commercial and ideological tracking and data mining. Just how little can be expected from governments regarding data protection became clear on June 28, 2012, when the German Bundestag passed new legislation allowing the state to sell its citizens' data to advertising and credit agencies as long as citizens did not opt out by filing an objection. This resolution was made in an almost empty parliament as the twenty-first item of its agenda, shortly before 9 pm, just after the beginning of the European Cup semifinals, Germany vs. Italy. The vote passed by a narrow margin but was later annulled following the protest of data protectionists. However, the fact that a majority of two or three politicians can pass such a law does not leave much room for consolation.

Is privacy better protected in the world of business? We might suppose so, given that its primary goal is not control or moral judgment but selling, satisfying whatever demand it perceives. However, for this very reason business is even more inquisitive than intelligence agencies, which are only concerned with potential threats. The transparent customer is the larger and weightier twin of the transparent citizen. Marketing consultants dream of the "full take" just as profoundly as intelligence agencies—if not more so—and of the real-time mining of social media, online communication, and offline actions. Among other things, they dream of the supermarket equipped with intelligent path tracking, that is, how a customer navigates the store based on data captured from their mobile. Via RFID chips feeding and coordinating biometric data the "smart" supermarket also registers, for example, whether a customer puts cream cheese back onto the shelf and opts for low-fat cottage cheese instead. Knowing his or her preference, the supermarket will now highlight diet products as the customer walks by and will also adjust in real time, assuming his willingness to pay more for less fat, the prices on the electronic displays.[3] Marketing loves data retrieval that allows for the refinement of the classical concept of segmentation as customization for the individual consumer.

The transparent customer is always also a transparent citizen. This justifies Morozov's concern that companies could be forced by governments to share their data. Morozov demands more than legislation in order to control IT companies. He maintains that it is necessary to take action to prevent a "data catastrophe" comparable to that envisaged by the ecological movement. At a certain point one's energy bill was no longer simply a private matter since the ecological consequences of individual energy consumption affects everyone. Analogously, our dealings in personal data have a public ethical dimension. Morozov is not only targeting the extrospective variant of self-tracking, that is, the saving and sharing of data that directly affects others (via camera, audio recording, or tagging in social media). Already the introspective variety—the gathering of personal data by insurance companies concerning driving or consumption habits, physical exercise, movement and mobility, and so on—presents a problem. It contributes to the determination of statistical criteria and norms against which all customers, regardless of their willingness to disclose private data, will be measured. Every purchase of an intelligent trash container increases the pressure on all those who do not yet cooperate with the data-collecting servants of the municipal garbage collector. Morozov's cautionary conclusion is that individual generosity—or perhaps promiscuity—with data sets the standards from which others will be unable to extricate themselves.

Morozov's perspective approaches the "ethics of responsibility for distant contingencies" demanded by Hans Jonas in his 1979 book *The Imperative of Responsibility: In Search of an Ethics for the Technological Age*. We have to consider the consequences of our actions even though they do not affect us or our immediate environment directly.[4] At the same time, Morozov's perspective points to the problem of surveillance, underlining just how complex the subject is as soon as one delves into it more deeply.[5] This approach turns the victims themselves into perpetrators while signaling the inefficacy of legal action vis-à-vis more complex and ambivalent ethical discussion. No wonder that others have pointedly recast Morozov's intimation of a structural problem within information society as a matter of politics. Among the reactions to Morozov's contribution in the *Frankfurter Allgemeine Zeitung* one could read that total surveillance is an insult to democracy, that mature citizens were being treated like immature children, and that the protest should not be seen in terms of the ecological movement but rather as comparable to the 1960s resistance against "emergency legislation." The political inflection of discussion was echoed in the appeal of Gerhart Baum, the former interior secretary from the Free Democratic Party: "We lack a citizen's movement for the protection of privacy as it existed and exists for the protection of natural resources."[6] Only the late chief editor of the *Frankfurter Allgemeine Zeitung* Frank Schirrmacher noted—and more than once—that the general sense of alarm in the wake of Snowden's revelations did not result from the disclosure of sophisticated surveillance technologies but from the realization that those technologies apply the same logic, systems, formulas, and mechanisms that determine our everyday life and working environment. Elsewhere, Schirrmacher, speaking about GPS, points out that the intercommunication of the giants of Silicon Valley and the intelligence agencies has not come about in a dystopian, Orwellian mode but "by way of things that even please us."[7] This fusion between what we fear and what we desire is the problem that paralyzes politics and people.

Morozov's correlation of environmental and data catastrophe, which meanwhile has gained some notoriety, is, in the end, unsound. When speaking of data catastrophe, the principle of a shifting baseline—as used in the discourse of the environmental catastrophe—is not equivalent to the destruction of the natural resources for future generations. The data catastrophe "only" threatens current cultural norms, and by contrast with global warming and pollution, a disaster resulting from altered values applied to social coexistence is hardly guaranteed. While the ecological movement's call to halt in response to the looming end of mankind can hardly be contradicted (the focus of contention being only a matter of the urgency of its appeal), saying "Halt" to cultural change would seem to oblige future generations to observe established norms of social interaction.[8] When motivated by cultural concerns, an ethics of preservation is less convincing than when it is a response to the known threat of environmental catastrophe. Not only must a culturally inclined ethics of preservation substantiate the reality of a threat; it must also speak to its menacing character, all the while resisting the counterargument that radical upheavals of culture are inherent within modernity.

The data catastrophe demands a more profound discussion than that surrounding questions of how to retain the integrity and privacy of mail in the age of digitization. It points to a change of social mentalities chiefly embodied in digital natives. The fact that this constituency appears unbothered by the loss of their private sphere is for many—and especially for members of the older generation—evidence of ignorance and indifference. From a psychosociological perspective, the lack of protest might also be understood as an emancipatory effort—as a longing for a realm that no longer differentiates between the private and the public, or as a rebellion against parents and grandparents whose earlier cultural revolution, which involved—in the 1960s and 1970s—making the private sphere public, has now become further radicalized with the help of the new media. On the one hand, this rebellion may be seen as very successful, given all the complaints of the older generation concerning the youthful lack of concern. On the other hand, this longing may simply be a resurgence that can be referred back to historical models since, in the early twentieth century, transparent man was not only invoked by communists against bourgeois culture but also by the Western avant-garde.[9] The guiding principles of other earlier cultural tendencies—best expressed in Georg Simmel's declaration "The secret is one of man's greatest achievements" as well as in Peter Handke's admission "I live off of what the others don't know about me"[10]—lose their validity under the contemporary imperative of transparency and disclosure, to say nothing of the fact that they prove to be impracticable against the prospects of intelligent things and smart environments. From this perspective, surveillance and control are merely the social implementation of the radical transparency widely propagated and practiced in social networks.

Compared to the ecological catastrophe, as an existential problem the data catastrophe is less menacing and as an ethical one less unequivocal. It is possible that this is the reason that Morozov's discomforting but entirely necessary call for a larger debate to counteract our data-specific ignorance has proved ineffective. Perhaps it explains the appeal of the emancipated-citizen-versus-suppressive-state rhetoric, which was made all the more persuasive when the British government blundered in sending its Secret Intelligence Service to the *Guardian*'s offices in order to destroy the hard disks holding Snowden's information. With this purely symbolic act of power—no intelligence agency worthy of its name believes that in the age of digital reproduction unwanted data can be erased through material violence—the media circle was strategically closed at the point where it had begun, namely with Edward Snowden's "betrayal." Although many have rightly regarded this betrayal as more of an awakening and as a call to necessary debate, in most cases the discussion does not go beyond the consequences that Snowden himself attributed to his disclosures. It is easy to understand why.

5

COLD CIVIL WAR

The hypothetical future report relating the events of the NSA affair and Snowden's betrayal will probably be ambivalent about listing Snowden among the heroes of history not because his deed was evaluated differently even by former U.S. presidents but because his purported heroism was based on a romantically glorified view of society. As Snowden declared in his interview with the *Guardian* in July 2013 and his TED talk in March 2014, he had wanted to inform the world about the snooping programs so that it would have the chance to do something to counteract it. He saw himself as a scout and trailblazer for change, someone with no doubt that his conscience would exonerate him for breaking any oaths of office that had been in the way of the truth. He believed in martyrdom, in giving up his own life for the public good. And indeed, Snowden is a contemporary version of the David and Goliath myth, attesting to the power of the individual in the face of the most powerful of nations, an example of the fact that, outside the academic system, certain discursive controversies can be launched and addressed with greater impact—something that critical scientists have been zealously working toward with little success.

The ambivalence of Snowden's heroism is not connected with his optimistic belief in the good of people but in its claim for some kind of ownership of the Internet. This gesture can be seen in the title of his TED talk: “Here Is How We Take Back the Internet.” Who is talking? How many of *us* are there? How can they reserve the right to determine the fate of a medium? When we reduce the problem of data protection to the snooping of intelligence agencies, it may be plausible to demand restitution, and the questions above may appear to have obvious answers. But if one sees the “ideology of ‘information consumerism,’” as Morozov puts it, as part of a social development, the question arises: Through what mandate—and with what chance of success—do activists wish to dictate the development of a medium that they do not own? To be clear, my question is aimed at the logic of the argument and in no way indicates any dismissal of the demands arising. On the contrary, the hope is that by addressing its cultural and social roots the problem will be tackled more rigorously. What renders Snowden’s heroism critically ambivalent is the superficiality of the debates it has incited, sometimes even soliciting the help of those who have internalized the ideology of data consumption while preaching it with their products: the software developers and data miners.

We cannot exclude the possibility that some software developers will be sensitized by the discussion of data protection and will refrain from the unnecessary retrieval of user data when they program their next app. It is conceivable that privacy could be prized above the economic considerations of data accumulation. However, given the increasing role that big data is playing in the economy, one cannot expect many startups to abstain voluntarily from data mining—not unless the payoff manifests itself as a competitive advantage in the form of consumer preference. Here lies a potential that has been initiated by the debates. In the realm of digital media it is possible that a parallel market will develop that values the protection of customer data over the profit to be made from data capture. An “organic Internet,” so to speak, whose products would be relatively more expensive, as are vegetables without pesticides and meat from happier chickens. Such a market might undermine, from an unexpected direction, the fiercely contested arguments for net neutrality—data transmission independent of form, content, sender, and the reputation or spending capacity of the receiver—possibly stirring net activists into more protests. The problems facing a two-class Internet, however, are not greater than those of the divided food market. On the contrary. With regard to food, the reasons some people decide to buy a less safe product are purely economic, whereas on the apps market the choice could also be made on the basis of conviction. In any case, the discussion will advance these economic and ideological questions instead of remaining stalled in the legal mire that Snowden has brought it to.

Limitations of the ongoing discussion are illustrated by a survey of ten "pioneers and theoreticians of the Internet" featured in the weekly newspaper *Die Zeit* on the question: "Can the Internet Be Saved?"[1] The answers are rife with militancy and only occasionally show any deeper awareness of the true problems. For example, Markus Beckedahl, the operator of the blog netzpolitik.org, writes: "Nothing less than our digital future with the basic values and rights that we know and have learned to love is at stake." And in a similar vein Anke Domscheit-Berg, a net activist and leading candidate of the Brandenburg Pirates Party in the governmental elections, urges: "We can continue pretending to be blind and deaf, and we will find ourselves in a world in which we will attempt to explain to our children that, at one time, there was a free Internet and how, when it ended, many other elements of freedom disappeared forever. But we can also powerfully revolt and reclaim with tooth and claw the Internet as we once knew it." Love, teeth, claws—an honorable protest against the course of events that nevertheless ignores the extent to which the early Internet carried its current structure within itself all along. The old aspiration—given up in the meantime by most net theoreticians—of the Internet as a place of free and liberating communication rested from the beginning on a misunderstanding; it is a misperception of the net as something existing independently of the computer. Advocates underlined all the possibilities of networking and overlooked the requirements of calculation that computation imposes on the human condition the more it provides links from computer to computer. Networked computers want to measure and calculate everything just as much as they want to copy everything. With regard to copying, the answer for many—and mainly for net activists—is to say goodbye to the copyright rules of the analog world. The same applies to privacy. Measuring and transparency are the end-all of the be-all. Here also clinging to past customs does not help.

In this light, Viktor Mayer-Schönberger, a coauthor of the book *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (2013), answers in the same survey much more to the point and without illusions: "In a nutshell this is the new task of governments—the all-encompassing, provisional control of society, based on information. And yet, governments are late-comers. They follow businesses like Google and Facebook and organizations like Wikipedia (and WikiLeaks!) that have recognized this much earlier. This is not the end, this is only the beginning." Cybernetics—no teeth or claws will help here—has always been the cover-up for a control to which more and more aspects of human life are now subjected through the Internet—of both people and of things. It is obvious that governments will use these new affordances in order to fulfill their tasks more effectively, and the political discussion will hardly question this. In most cases it will insist only that data mining take place in a transparent and democratic way. The instruments of control should be visible (with the welcome side effect that self-disciplining will result), and they should be accessible to everyone (which, considering the true cost of complex data analysis, can hardly be realized).[2]

In his "Postscript on the Societies of Control" Gilles Deleuze illustrates a future city "where one would be able to leave one's apartment, one's street, one's neighbourhood, thanks to one's (dividual) electronic card that raises a given barrier." Twenty years later this prognosis has been realized in products like the NFC Ring, which opens locks, or the Nymi wristband, which uses one's personal pulse rate as a means of identification. At the same time, what for Deleuze is the dystopian aspect of his scenario is also realized: "but the card could just as easily be rejected on a given day or between certain hours; what counts is not the barrier but the computer that tracks each person's position—licit or illicit—and effects a universal modulation."[3] Despite knowing that IBM has created a control room in Rio de Janeiro in which the feeds from all surveillance cameras are concentrated or that China is building similar control rooms in its new cities, one should not paint the future with old conceptual brushes. In the end there will be no Big Brothers to be dragged out of their control centers. There will be no live controllers who will activate or deactivate the cards. These cards will obey algorithms fed by the all-but-limitless collections of data that we have ourselves given up freely. The term for this has already been coined: "algorithmic regulation." Its congenial genius is "datafication," the transformation of communications and activities into quantifiable, tabulated data. The transition from a society of discipline into one of control, as announced in political philosophy, is implemented through the digitization of society. Datafication guarantees its execution by way of cybernetics.

More than forty-five years ago another, older branch of political philosophy already revealed many problems of society's adaptation to the logic of cybernetics under the heading "technocratic rationality." Its perspective, supposedly, replaces the authoritarian state, which leads to an end of discursive controversy. The realization of a normative moral order, which is "a function of communicative action oriented to shared cultural meaning and presupposing the internalization of values," is "increasingly supplanted by conditional behavior."[4] Bourgeois and socialist ideology thus gives way to an ideology determined by technology and science as "self-reification of men under categories of purposive-rational action and adaptive behavior."[5] The problem—as elucidated by Jürgen Habermas expanding on Max Weber's and Herbert Marcuse's criticism of rationality—is the transformation of rationality itself from a means of emancipation for mankind into a means of its reification. Max Horkheimer and Theodor Adorno have described this aspect of the process of modernization in their *Dialectic of Enlightenment* (1944), and Zygmunt Bauman has dealt with it as "dialectic of order" in his *Modernity and the Holocaust* (1989). In each case, instrumental rationality—albeit with different levels of cruelty—creates a situation of "moral mercilessness" in which people no longer feel responsible for existing rules of behavior nor feel the need to challenge them; they simply follow and enforce them with an august sense of obligation. Adiaphorization—the technical term in ethics for when people do not feel responsible any longer for the effects of their actions—becomes redundant (or is hiding behind the interface) when it is no longer a person but the algorithm (as the new, perfect "brother Eichmann") who sets the rules and enforces them.

In a recent book on *Liquid Surveillance: A Conversation* (2012), Bauman pointed out the danger of outsourcing moral responsibility to technological developments: "We no longer develop techniques 'in order to' do what we want to be done, but we select things for doing just because the technology for doing them has been developed (or, rather, has been come across; accidentally—'serendipitously'—found)."[6] The question of where these technologies come from, supplying us with parameters of action, and of how the inventive spirit and the profit orientedness of young programmers cohere, will be discussed later. Let these following cautionary words—from a similar statement on the automatic link between technological possibility and practical usage in Hans Jonas's abovementioned book on responsibility—suffice for now. For Jonas the fate of man lies in the "triumph of *homo faber*," which makes him into "the compulsive executer of his capacity." As Jonas states: "If nothing succeeds like success, nothing also entraps like success."[7] We have given in to this technological success more than ever. The modern terms for this are computing, programming, deploying algorithms.

The submission to what is technologically possible—both trumpeted and deplored—also explains why there is such interest in analyzing the behavioral patterns of employees and how they communicate, with solutions offered by companies such as Sociometric Solutions, Hitachi, and Evolv. E-mail filters, data mining, sociometric badges, and other methods and devices that analyze internal company communications, cooperation, and movements may throw up red flags for union activists and privacy advocates. However, the aim of optimizing the working process in order to "develop a more productive, more positive and more profitable workforce" and "to drive increased employee satisfaction, retention, productivity and engagement"—which Evolv states as its mission—does not sound unreasonable. After all, how can you deny employers the right to know what their employees are doing during paid work time? But this may already be the wrong question. The fact is that they want to know as much as they can—as the software engineer Ellen Ullman illustrates in her 1997 *Close to the Machine: Technophilia and Its Discontents.* She recalls the owner of a small insurance business who wanted her to help him record all his office manager's keystrokes: "You can count every keystroke, and you want to count them simply because it's possible. You own the system, it's your data, you have power over it; and, once the system gives you this power, you suddenly can't help yourself from wanting more." Technology creates desire; its options are no option for us: "We think we are creating the system, but the system is also creating us. We build the system, we live in its midst, and we are changed."[8] Ullman's conclusion confirms Bauman's and Jonas's warnings that media have their own agenda. As previously stated in words usually attributed to the Canadian media theorist Marshall McLuhan: "We become what we behold. We shape our tools and then our tools shape us."

If, in the context of the NSA affair, placards blazoned with "YES WE SCAN" appeared in demonstrations during the summer of 2013, they were pointedly referring to President Obama's election slogan "YES WE CAN," expressing their disappointment in him and his policies. The conceptual and actual rhyme of these two slogans—we scan because we can—simultaneously articulates the fatalistic activism that for Jonas and Bauman characterizes the relationship of modernity and technology. Yes, we can collect all kinds of data, and we can analyze them—and therefore we do it. The "full take" that the intelligence agencies are aiming for is no contradiction in modern society; it is a part of its inherent contradictory nature. Control society and the *Culture of Control*—the title of a 2001 book by David Garland—are the consequences of processes of modernization that, if nothing else, apply all available technologies to improve ever more effective methods of organization and control.

The contradictory nature of the modern era has also ensnared its powerless populations. Pragmatic considerations have led to an unsolicited provision of data simply for the sake of comfort and the thirst of knowledge, as can be seen from the example of contemporary human interaction with self-tracking and smart things. During the NSA scandal one could observe that the lack of protest might be explained differently. This lack was a function of a "longing for surveillance" in the sense of being taken care of or looked over in a modern world that has become confusing, and also of a "*love* of being seen" in the sense of "I am seen (watched, noted, recorded), therefore I am."[9] Both motives—exhibitionism as self-assurance and the desire for order as a reduction of complexity—are psychologically comprehensible—as is the thirst for knowledge and comfort. Potentially, this makes the individual into an ally of monitoring and control.

When, also in the context of the NSA affair, there is talk of a "cold civil war,"[10] the conflict should not be seen as reducible to one between citizen and state, or as a war between digital natives and digital immigrants, or between those who buy and sell data or illegitimately acquire data and all the others. The civil war is taking place not between the citizens but *within* the citizenry, that is, between the interest in technological progress, orientation, and being noticed on the one hand and, on the other, the occasional sense of discomfort at being the object of surveillance and control. This internal civil war hinders all attempts at strengthening data protection through, for example, a system of decentralized data storage in individual routers and servers. Although this would weaken the data octopuses of the Internet by exploiting the Internet's fundamentally decentralized structure, it would also rob the citizenry of many advantages that are a result of the centralization and interconnection of data. The question that needs to be untangled is this: To what extent can modern society resist the allure of new inventions and the advantages that they promise?

If such resistance does not succeed, future histories may report on this dispute as follows: In 2023 the German Ministry of the Internet (MOTI), which had been created shortly after Snowden's disclosures, took out an injunction against the Association of Activists of Data Protection (AADP). Their so-called white block had long ago demanded—by referring to Gilles Deleuze and other critics of the cybernetic control society—the creation of "vacuoles of noncommunication" as "circuit breakers,"[11] an example being the deactivation of GPS tracking on smart phones. Although by 2023 it was no longer possible to deactivate GPS tracking, owning a smart phone with a "presence tag" was not yet mandatory. Changes were proposed by MOTI because the Department of Transportation was planning to require presence technology for traffic regulation (with a location precision of five centimeters). This was particularly important because by this time all driven vehicles were virtually soundless. Collisions could be avoided through this technology, even for the deaf or blind, by automatically triggering warning signals or braking commands for two presence-tag carriers whose locational coordinates fell below the distance limit. This technology, which was regarded as absolutely secure, could scarcely be refused by the data-protection activists, but they nevertheless demanded anonymization. After all, preventing a collision between a car and a bicycle, for example, did not require the identification of the drivers. The Ministry of the Internet did not share this point of view, reasoning that given the data available concerning the physical and psychological condition of the drivers, their everyday routines, the car models, and many other factors, state-of-the-art data mining could help calculate the probability of a collision and allow the enforcement of appropriate preventive measures in an even more timely manner. They argued that since traffic safety was not a private matter, no citizen should be allowed to remain anonymous in this instance. The demand to create barriers in the way of cybernetic communication was regarded as dangerous, and even as terroristic by some, and therefore it was forbidden by law.

NOTES

PREFACE

1. http://nextconf.eu/next11/next11-means-data-love (no longer online; grammar issues in the original).
2. The terms "data" and "information" do not differ quantitatively, as is suggested when referring to a bit of data as a "piece of information," but qualitatively. Data (as givens or facts; *datum* in Latin) embody the lowest level in the chain of perception, preceding both information (as processed data; *informare* in Latin) and knowledge (as interconnected information or a "serial event of cooperation and collaboration," in the formulation of Manfred Faßler, *Der infogene Mensch. Entwurf einer Anthropologie* [Munich: Wilhelm Fink 2008], 281, stressing the processual character of knowledge). From the perspective of perception theory, however, it is questionable that data (as givens before interpretation and the construction of meaning) exist for the observer. As an alternative to "data," the suggestion has been made to use "capta" (from the English "to capture") in order to keep in one's mind the inevitable "taking" of the given. See Johanna Drucker, "Humanities Approaches to Graphical Display," *Digital Humanities Quarterly* 5, no. 1 (2011), http://www.digitalhumanities.org/dhq/5/1/000091/000091.html. This term, though, subverts the difference between data and information (as *processed* data). Since the purpose of this book is not a terminological discussion, it may suffice to keep in mind the indicated difference among data, information, and knowledge.
3. http://www.datalove.me; http://www.datalove.me/about.html.

1. INTELLIGENCE AGENCY LOGIC

1. *Welt am Sonntag* (July 28, 2013), http://www.welt.de/print/wams/article118447661/Steinbrueck-dankt-Edward-Snowden.html); Wort.lu (September 20, 2013), http://www.wort.lu/en/view/thank-you-mr-snowden-says-eu-s-reding-523bdfa4e4b0c159be9abbba.
2. *Huffington Post* (July 18, 2013), http://www.huffingtonpost.com/2013/07/18/jimmy-carter-edward-snowden_n_3616930.html.
3. *Der Spiegel* (July 27, 2013), http://www.spiegel.de/politik/deutschland/nsa-ex-innenminister-schily-haelt-furcht-vor-ueberwachung-fuer-paranoid-a-913507.html.

2. DOUBLE INDIFFERENCE

1. See the lecture by the political scientist Christoph Bieber, "Politik und Staat im Netz. Social Media nach dem NSA-Abhörskandal und der Wahl in Deutschland" (Politics and state on the net: Social media after the NSA phone tapping scandal and elections in Germany), one in the series *Digital Media Studies in der Praxis. Wie die Geisteswissenschaften auf die neuen Medien reagieren* (Practical digital media studies: How the humanities react to the new media), which I organized at Basel University on September 24, 2013. Gerhart Baum compares it to Fukushima in an article in the *Frankfurter Allgemeine Zeitung* (September 24, 2013), http://www.faz.net/aktuell/feuilleton/gastbeitrag-von-gerhart-baum-ich-will-dass-wir-beissen-koennen-12589869.html.
2. http://nikeplus.nike.com/plus/what_is_fuel.
3. Frank Schirrmacher, "Digitale Autonomie. Europa 3.0," *Frankfurter Allgemeine Zeitung* (July 4, 2013), http://www.faz.net/aktuell/feuilleton/digitale-autonomie-europa-3-0-12271068.html.
4. Chris Chesher, "Colonizing Virtual Reality: Construction of the Discourse of Virtual Reality, 1984–1992," *Cultronix* 1, no. 1 (1994), http://cultronix.eserver.org/chesher.

3. SELF-TRACKING AND SMART THINGS

1. Evgeny Morozov, "Information Consumerism: The Price of Hypocrisy," *Frankfurter Allgemeine Zeitung* (July 24, 2013), http://www.faz.net/aktuell/feuilleton/debatten/ueberwachung/information-consumerism-the-price-of-hypocrisy-12292374.html.

2. This is the introductory sentence on a website for tracking sleeping patterns. http://www.selftrackinghq.com/zeo.
3. This is a quote from a devoted self-tracker in Klint Finley's article "The Quantified Man: How an Obsolete Tech Guy Rebuilt Himself for the Future," *Wired* (February 22, 2012), http://www.wired.com/wiredenterprise/2013/02/quantified-work/all.
4. Zygmunt Bauman and David Lyon, *Liquid Surveillance: A Conversation* (Cambridge: Polity, 2013), 71. Bauman is referring to John Burnham's *The Managerial Revolution* (New York: John Day, 1941).
5. Gary Wolf, "Know Thyself: Tracking Every Facet of Life, from Sleep to Mood to Pain, 24/7/365," *Wired* (June 22, 2009), https://archive.wired.com/medtech/health/magazine/17-07/lbnp_knowthyself?currentPage=all.
6. Jamin Brophy-Warren, "The New Examined Life: Why More People Are Spilling the Statistics of Their Lives on the Web," *Wall Street Journal* (December 6, 2008), http://online.wsj.com/article/SB122852285532784401.html.
7. The first example was the subject of a discussion at the Quantified Self conference in 2011 in Mountain View, California. See Emily Singer's report on the conference, "'Self-Tracking' für ein besseres Leben" (Self-tracking for a better life), *Technology Review* (June 15, 2011), http://www.heise.de/tr/artikel/Self-Tracking-fuer-ein-besseres-Leben-1259259.html. The second example was reported by Julia Friedrichs in her article "Das tollere Ich" (The super me) in the magazine of the weekly *Die Zeit* (August 8, 2013), http://www.zeit.de/2013/33/selbstoptimierung-leistungssteigerung-apps.
8. Gary Wolf, one of their protagonists, underlines exactly this altruistic aspect of self-tracking: "Oddly, though, self-tracking culture is not particularly individualistic. In fact, there is a strong tendency among self-trackers to share data and collaborate on new ways of using it. People monitoring their diet using *Tweet What You Eat!* can take advantage of crowdsourced calorie counters; people following their baby's sleep pattern with *Trixie Tracker* can graph it against those of other children; women watching their menstrual cycle at *MyMonthlyCycles* can use online tools to match their chart with others'. The most ambitious sites are aggregating personal data for patient-driven drug trials and medical research. Self-trackers seem eager to contribute to our knowledge about human life." Wolf, "Know Thyself."

9.Helga Nowotny, “Wissenschaft neu denken. Vom verlässlichen Wissen zum gesellschaftlich robusten Wissen,” in *Die Verfasstheit der Wissensgesellschaft*, ed. Karsten Gerlog and Anne Ulrich (Münster: Westfälisches Dampfboot, 2006), 27, 33.

10. See Morozov, “Information Consumerism.”

4. ECOLOGICAL DATA DISASTER

1. Regarding this future project at the University of Newcastle, see “Smile, You’re on BinCam! Five Households Agree to Let Snooping Device Record Everything They Throw Away,” *Daily Mail* (March 4, 2011), http://www.dailymail.co.uk/news/article-2000566/Smile-Youre-bin-cam-The-snooping-device-record-throw-away.html.
2. Evgeny Morozov, “Information Consumerism: The Price of Hypocrisy,” *Frankfurter Allgemeine Zeitung* (*FAZ*) (July 24, 2013), http://www.faz.net/aktuell/feuilleton/debatten/ueberwachung/information-consumerism-the-price-of-hypocrisy-12292374.html.
3. This example is reported, with reference to the German company Metro Group, by Andreas Weigend, former chief scientist at Amazon, in his talk“The Social Data Revolution: More Efficient Than the KGB?”at the World Innovation Forum, New York (May 8, 2010), http://fora.tv/2010/06/08/Andreas_Wigend_Marketing_and_Web_20/The_Social_Data_Revolution_More_Efficient_than_the_KGB. Four years later, Apple’s iBeacons sensor promised such “location-based marketing,” possibly starting a trend, as it did with the iPhone.
4. Hans Jonas, *The Imperative of Responsibility* (Chicago: University of Chicago Press, 1984), 26. Originally published in German in 1979.
5. Morozov expands on this complexity in “The Real Privacy Problem,” *MIT Technology Review* (October 22, 2013); and in his book *To Save Everything, Click Here: The Folly of Technological Solutionism* (New York: PublicAffairs, 2013).
6. Wolfgang Michal, “Überwachung und Verfassungsrecht. Die Kränkung der Demokraten,” *Frankfurter Allgemeine Zeitung* (August 5, 2013), http://www.faz.net/aktuell/feuilleton/ueberwachung-und-verfassung-srecht-die-kraenkung-der-demokraten-12369328.html; Gerhart Baum, “Ich will, dass wir beißen können,” *Frankfurter Allgemeine Zeitung* (September 24, 2013), http://www.faz.net/aktuell/feuilleton/gastbeitrag-von-gerhart-baum-ich-will-dass-wir-beissen-koennen-12589869.html.

7. Frank Schirrmacher, "Politik im Datenzeitalter. Was die SPD verschläft," *Frankfurter Allgemeine Zeitung* (September 25, 2013), http://www.faz.net/aktuell/politik-im-datenzeitalter-was-die-spd-verschlaeft-12591683.html. See also Frank Schirrmacher on the Beckmann TV show *Der gläserne Bürger—ausgespäht und ausgeliefert* (July 18, 2013), minute 102.
8. The consensus between the views of the digital native Morozov (born 1994) and those of the digital immigrant Schirrmacher (born 1959) regarding the negative evaluation of today's developments in technology shows that cultural criticism or even pessimism cannot be attributed unproblematically to the older generation. Also Michel Serres (born 1930) shows with his book *Petite Poucette* (2012) that the older generation does not necessarily behave in a way that is motivated by cultural pessimism.
9. On this, see the paragraphs concerning Charles Fourier's social utopias, the glass architecture of the early twentieth century, surrealism, and Trotsky, in *Manfred Schneider. Transparenzraum* (Berlin: Matthes & Seitz, 2013).
10. Georg Simmel, *The Sociology of Georg Simmel*, trans. and ed. Kurt H. Wolf (New York: Macmillan, 1950), 330; Peter Handke, *Am Felsfenster morgens* (Salzburg, 1998), 336.

5. COLD CIVIL WAR

1. "Ist das Internet noch zu retten?" *Die Zeit Online* (August 8, 2013), http://www.zeit.de/digital/datenschutz/2013–08/internet-pioniere-nsa.
2. On the demand for transparency, see Tal Zarsky, "Mining the Networked Self," *Jerusalem Review of Legal Studies* 6, no. 1 (2012): 120–136; Tal Zarsky, "Transparent Predictions," *University of Illinois Law Review* 4 (2013): 1503–1569.
3. Gilles Deleuze, "Post-Scriptum on the Societies of Control," *October* 59 (Winter 1992): 6. https://sites.google.com/site/deleuzemedia/textes/post-scriptum-sur-les-societes-de-controle.
4. Jürgen Habermas, "Technology and Science as Ideology," in *Towards a Rational Society: Student Protest, Science, and Politics*, trans. Jeremy Shapiro (Boston: Beacon, 1979), 107.
5. Ibid., 106.
6. Zygmunt Bauman and David Lyon, *Liquid Surveillance: A Conversation* (Cambridge: Polity, 2013), 86. See Klint Finley, "The Quantified Man:

How an Obsolete Tech Guy Rebuilt Himself for the Future," *Wired* (February 22, 2012), http://www.wired.com/wiredenterprise/2013/02/quantified-work/all.

7. Hans Jonas, *The Imperative of Responsibility* (Chicago: University of Chicago Press, 1984), 26.
8. Ellen Ullman, *Close to the Machine: Technophilia and Its Discontents* (New York, 2012), 98, 91. Anna North presents these quotes in her article "When Technology Makes Work Worse," *New York Times* (August 19, 2014). North also refers to Rhodri Marsden's text "Is Your Boss Spying on You?" *Independent* (March 19, 2014). Marsden concludes that the results of such analyses "could eventually produce data sets that cover the entire career of an individual, following us from job to job and depriving us of the opportunity to creatively airbrush our past within the context of a one-page CV." http://www.independent.co.uk/life-style/gadgets-and-tech/features/is-your-boss-spying-on-you-9203169.html. From a management perspective the transparent employee is desirable exactly for the reason that it prevents such airbrushing. The morals—this is the paradoxical and absurd aspect of such analyses—are on the side of those who want to reveal, not to conceal, the truth. For Evolv's self-description, see www.linkedin.com/company/evolv-on-demand.
9. The first quote is by David Lyon in Finley, "The Quantified Man"; the second quote is by Zygmunt Baumann in Baumann and Lyon, *Liquid Surveillance*, 168, 130.
10. See Iljia Trojanow, "Die Kollateralschäden des kalten Bürgerkriegs," *Neue Zürcher Zeitung* (August 2, 2013), http://www.nzz.ch/meinung/uebersicht/die-kollateralschaeden-des-kalten-buergerkriegs-1.18126416.
11. "Control and Becoming" (Gilles Deleuze in conversation with Antonio Negri), http://www.uib.no/sites/w3.uib.no/files/attachments/6._deleuze-control_and_ becoming.pdf. Gilles Deleuze, *Negotiations, 1972–1990* (New York: Columbia University Press, 1995), 175.

6. DATA-MINING BUSINESS

1. For details concerning the calculation, see http://klout.com/corp/klout_score.
2. Alfred W. Crosby, *The Measure of Reality: Quantification and Western Society* (Cambridge: Cambridge University Press, 1997).