

# Chapter 7

## Epilogue: Digital Roads to Totalitarianism



### 7.1 Digital Emancipation

The digital revolution was meant to emancipate. In the *Declaration of the Independence of Cyberspace* from 1996, John Perry Barlow declares the new digital reality, Cyberspace, to be an independent new world of freedom and equality without oppression of the old world of nation-states ruled by governments. Barlow compares the digital revolution to the American War of Independence and the pioneers of digitalization to the heroes of the American Revolution: "... those previous lovers of freedom and self-determination who had to reject the authorities of distant, uninformed powers."<sup>1</sup>

The digital reality that came to pass the following years and we are now in the midst of is far away from the digital utopia of liberation and self-determination. The Internet and the digital technology may just as well pave ways for new forms of oppression and dominion. Instead of being a force of democratization and emancipation, the digital revolution may turn out being the opposite and contribute to undermine democracy and political self-determination.

---

<sup>1</sup>John P. Barlow (1996): A declaration of the independence of cyberspace. Verified January 7, 2018 <https://www.eff.org/cyberspace-independence>

The Arab Spring in 2010 is an example of an event where the Internet and social media played an empowering and emancipatory role for citizens by providing a communicative infrastructure for the uprisings the authorities did not control. In Tunisia Facebook took hold as the “revolution headquarters” and in Egypt it served as online incubator of a revolutionary youth movement that could mobilize and organize protests (Herrera 2015). Four years after the uprising, tables have turned. In Egypt the military regime began in 2014 the so-called Social Networks Security Hazard Monitoring System operation, which is a surveillance program informing the regime of the whereabouts and communication of citizens much more efficiently than during the former authoritarian regime: a tool for emancipation and protest is turned into a tool of repression and social control.

It is not only democracy and self-determination on the political level that run the risk of being disrupted by the digitalization. In the end, the digital revolution may result in an elimination of autonomy and free will of the individual. Too much information may be a greater threat to freedom than misinformation. A digitalized too factual and too informed society may amount to a new form of digital totalitarianism. The lack of trust that fuel post-factual tendencies may be the least of problems compared to a data-driven factual society where trust is eliminated as phenomenon and replaced by control. It is on its way in China.

## 7.2 The Chinese Panopticon

In 2014 the State Council in China announced and initiated the construction of the *Social Credit System*, an ambitious project with the official purpose of generating “honest mentality,” fostering a “culture of sincerity,” and raising the “level of trustworthiness in the entire society.” This is an important step toward building a “harmonious socialist society” and stimulating “the progress of civilization” in words of the offi-

cial document.<sup>2</sup> The system is under construction, the details are not yet in place, and participation will first be mandatory for every citizen and company in China from 2020 onward. Nevertheless, test versions already running locally and statements from those responsible for the implementation draw a picture of what is in the making: a surveillance society made possible by the digital revolution that enables monitoring and disciplining of the citizens by constantly providing incentives to conform to desired behavior.

The baseline is a rating system. Every citizen and company will have an account for social credit points and the score will determine the trustworthiness of the particular individual or company.<sup>3</sup> One's credit score will be decided automatically employing artificial intelligence for analyzing an enormous amount of data and information about the citizens. The information is gathered from many different sources of data like banks and financial institutions, stores, public transportation systems, Internet platforms, social media, and e-mail accounts. Not to forget the 570 million surveillance cameras with integrated facial recognition that are to be in place in 2020 with 170 million already up and running today (Fig. 7.1).<sup>4</sup>

Digitalization and the Internet have enabled such massive data collection that surveillance may be almost total with no angles out of sight or blind spots: an updated digitalized ver-

---

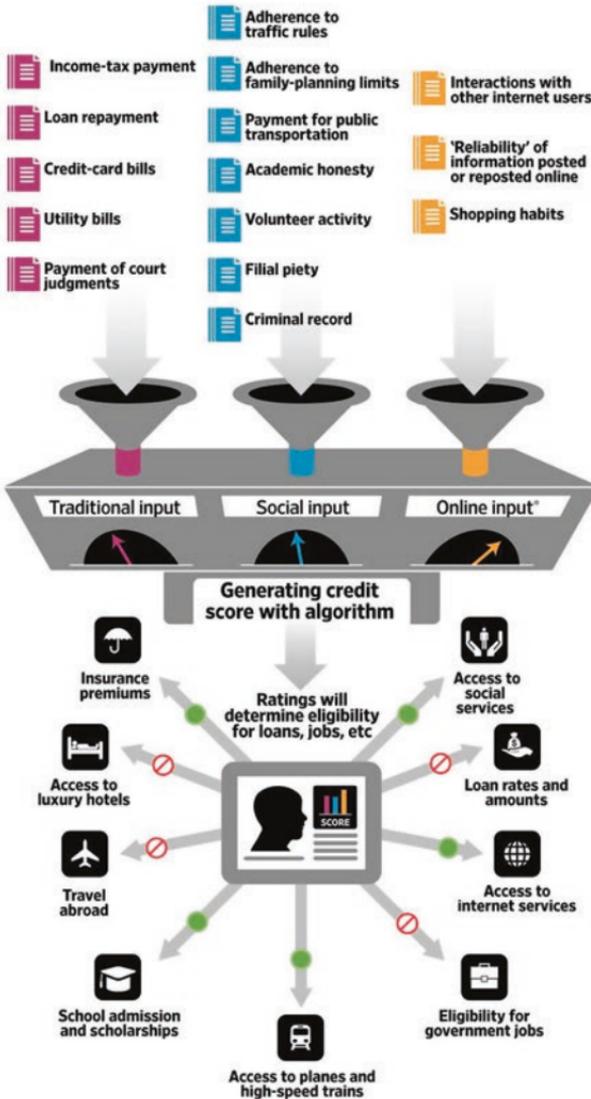
<sup>2</sup> [Planning Outline for the Construction of a Social Credit System \(2014-2020\)](#). Posted on June 14, 2014 Updated on April 25, 2015 State Council Notice concerning Issuance of the Planning Outline for the Construction of a Social Credit System (2014–2020), GF No. (2014)21. Verified 24.06.2017: <https://chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020/>

<sup>3</sup> Kai Strittmatter (2017): Creating the honest man. München, Süddeutsche Zeitung. Verified January 7th 2018 <http://international.sueddeutsche.de/post/161355280290/creating-the-honest-man>

<sup>4</sup> Chan, T.F. (2018). “Parts of China are using facial recognition technology that can scan the country’s entire population in a second,” *Business Insider*, 27.05.2018, verified 26.06.2018: <http://nordic.businessinsider.com/china-facial-recognition-technology-works-in-one-second-2018-3?r=US&IR=T>

### China Watching

Beijing wants to create a nationwide 'social-credit' system that compiles digital records of citizens' social and financial behavior to calculate a personal rating that will determine what services they are entitled to — and what blacklists they go on. Here's a look at how the system might work.



\* It is currently unclear how "online inputs" will be implemented. Source: WSJ reporting based on government blueprints, state-media reports and interviews with architects of the plan.

THE WALL STREET JOURNAL.

FIG. 7.1. Outline of the Social Credit System in China. (Source: *The Wall Street Journal*, 2016).

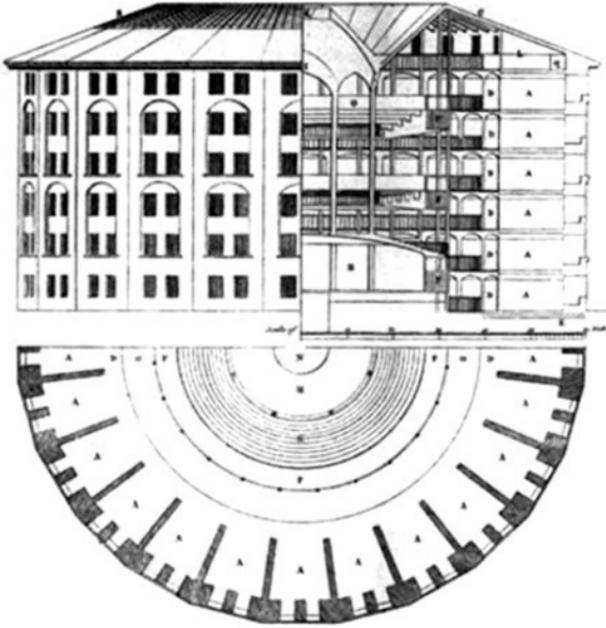


FIG. 7.2. Jeremy Bentham's original architectural plan for a *Panopticon*. A prison in which inmates are monitored constantly with no blank spots in the cells to hide from the Guards' gaze. (Wikipedia Commons. Verified 24.06.2018: [https://commons.wikimedia.org/wiki/File:Penitentiary\\_Panopticon\\_Plan.jpg](https://commons.wikimedia.org/wiki/File:Penitentiary_Panopticon_Plan.jpg)).

sion 2.0 of Jeremy Bentham's *Panopticon* ("all-seeing") where one's life is being monitored in detail 24-7 without any possible refuge from the gaze of the authorities. In the Panopticon, privacy is not an option (Fig. 7.2).

The Panopticon is employing surveillance to discipline the inmates to desired behavior. In Bentham's own words:

The more strictly we are watched, the better we behave.<sup>5</sup>

<sup>5</sup>Jeremy Bentham: unpublished, from the manuscripts of Jeremy Bentham in the Library of University College London. Leaflets on Bentham's Life and Work. Verified 24.06.2018: <https://www.ucl.ac.uk/bentham-project/publications/leaflets-benthams-life-and-work>

Surveillance contributes to discipline the surveilled (Haidt 2012). With surveillance and the information that results from it comes a disciplinary form of power (Foucault 1979). Monitoring and registering combined with rewards and sanctions for wanted and unwanted behavior is an efficient tool of *behavior modification*. Whether the surveillance takes place in institutions as prisons, schools, hospitals, the workplace, or the army or is generalized to the whole society, it aims at the same result: the production of obedient subjects who conform to what is expected and wanted by the authorities—normalized and law- and norm-abiding citizens.

The Social Credit System employs this panoptic power technique of surveillance-based discipline. The system monitors, registers, and rewards desired behavior with adding social credit points to one's credit score. Unwanted behavior, on the other hand, will cost points and lower the score. Voluntary community service, taking care of one's family, charity donations, and responsible consuming like buying diapers are point rewarding. On the other hand, if you, for instance, spend too much time and money on computer games, smoke in a nonsmoking zone, drop a cigarette bud, travel without ticket, drive recklessly, miss paying a bill in time, or spread fake news on social media, you lose points and the score drops. In one running version of a Social Credit System, Sesame Credit, an additional feature is that online friends on social media also count. Their score reflects on one's own providing an incentive to restrict one's relations to only model citizens deemed trustworthy. According to the 2014 plan, "reporting" others' breach of trust—as it is phrased—will also be rewarded.

Besides being publicly assessable for other citizens and their evaluation of one's character, the social credit score will determine one's economic and social opportunities and restrictions. It is decisive for whether one, for instance, may obtain a loan, get a job, enroll one's kids in a good school, or have access to public services. Social sanctions may also apply. Citizens with a low score risk being publicly exposed and shamed on billboards and social network sites as morally

flawed people, whereas those with a high score are presented and promoted as model citizens making it easier to find a partner. The score also decides one's freedom of movement. Restrictions that approximately 9 million Chinese with a low score experienced the hard way when they were denied booking tickets for domestic flights and high-speed trains. As the official catchphrase bluntly states:

Allow the trustworthy to roam everywhere under heaven while making it hard for the discredited to take a single step.<sup>6</sup>

It seems to work. Where the test versions are in operation locally, it has been reported that people's behavior and the social environment have changed for the better. The change of behavior results in the beginning from a conscious calculation and cost-benefit analysis: it pays off to behave well. After a while, though, the rules, regulations, and norms are internalized into an unconscious habit. As a citizen puts it: "At first, we just worried about losing points, but now we got used to it."<sup>7</sup>

Some even have the ambition and hope that it will work so well it is able to change human nature itself and create a new more honest and better human being and citizen. Zhao Ruying, who is in charge of the implementation in Shanghai, envisions that the system eventually will eliminate not only the need for punishment but also asocial *thoughts*:

We may reach the point where no one would even dare to think of breaching trust, a point where no one would even consider hurting the community. If we reached this point, our work would be done.<sup>8</sup>

If this goal is ever achieved, there will no doubt be social order and maybe even "harmony." The price to pay, on the

---

<sup>6</sup>Kai Strittmatter (2017): Creating the honest man. München, *Süddeutsche Zeitung*. Verified January 7th 2018 <http://international.sueddeutsche.de/post/161355280290/creating-the-honest-man>

<sup>7</sup>Mistreanu, S. (2018). Life Inside China's Social Credit Laboratory, *Foreign Policy*, 18.03.2018. Verified 24.06.2018: <http://foreignpolicy.com/2018/04/03/life-inside-chinas-social-credit-laboratory/>

<sup>8</sup>Ibid. (Strittmatter 2017)

other hand, is the actualization of a totalitarian Big Brother state that monitors, registers, and reprograms its citizens' behavior to total obedience with no space left for even unwanted thinking. Such a result, where even *thought crimes* are eradicated, would make even the leading members of The Party in the novel *1984* a little bit jealous.

Big Brother's methods of control have been updated. Even if China is not soft on crime, the Social Credit System employs power techniques of rewards and desire for happiness and success rather than fear, terror, and violence of old-school totalitarianism. Totalitarianism with a human face resembles *Brave New World* more than the brutality of *1984*. To condition and motivate may be a much more efficient way to produce obedient and conforming citizens than to repress through fear and terror. The new methods of sugar-coated digital control may show so effective they succeed in undermining critical thinking, autonomy, and self-determination. Not just in China.

The Chinese State Council is not alone in totalitarian dreams of total surveillance and control. It does not necessarily require an authoritarian state aiming at social order and harmony as *primus motor* to reach totalitarian conditions. An unregulated market for data and user information and the hunt for profits may be sufficient. Google is leading the way in a race and mission of colonizing, commodifying, and monetizing every aspect of our life.

### 7.3 Surveillance Capitalism

The same year China initiated the construction of the Social Credit System, 2014; on the other side of the Pacific Ocean in Silicon Valley, Hal Varian, chief economist at Google, held a speech addressing the great opportunities made possible by extraction of data combined with massive processing power. The speech revealed a vision for a future of a surveillance capitalistic society with no more room for privacy than in China. According to Varian, the elimination of privacy is the

(fair) price to pay, not for social order and harmony, but for the functionality, efficiency, and convenience of the products and services Google provides to the users. Gathering and analyzing information *about* the user is the condition for personalizing the products *for* the user. Privacy is exchanged for enhanced user experience and the convenience made possible by personalized optimization and customization of the products that automatically tailor them to the individual user. Only when Google knows at least your location, budget, and food preferences, it is able to provide a relevant suggestion for a restaurant nearby to have dinner. The more personal information Google possesses, the more efficiently and conveniently it is able to serve one's individual needs and demands. That is the basic justification of the surveillance. However, even more surveillance, data mining, and information gathering are necessary to realize the tech giant's vision. The ambition is that Google products should run so smoothly and conveniently for the user that it is not even necessary to *google* or ask Google questions. As company founder, Larry Page is quoted for saying:

[Google] should know what you want and tell it to you before you ask the question.<sup>9</sup>

Google should be able to predict our wants and desires before we have articulated them. To be able to do that, it needs to know us almost better than we know ourselves. That takes *a lot* of information. It also implies a total elimination of privacy. That is the necessary condition for mining the amount of data sufficient for knowing, predicting, and attending to our wants and desires before we have expressed them ourselves. For a company like Google, the right to privacy is an obstacle to their ambition and stated mission. To “organize the world’s information and make it universally accessible and useful”<sup>10</sup> taken literally implies a colonization and dispos-

---

<sup>9</sup>Hal R. Varian (2014): *Beyond Big Data*. Business Economics 49 (1)

<sup>10</sup>[Google.com/ about our company](https://www.google.com/about/our-company/). Verified 24.06.2018: <https://www.google.com/about/our-company/>

session of every bit of our private sphere and life: accessibility excludes privacy. For the right to privacy, Google CEO Eric Schmidt's defense for the surveillance practices is telling and chilling:

If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place.<sup>11</sup>

Google does not have an extended network of surveillance cameras to gather data and de facto implodes the difference between being online and offline into an *Onlife*, as in the Chinese surveillance society. Nor is it mandatory to use Google products. Nevertheless, the vast amounts of data necessary will increasingly be accessible through *the Internet of Things*. With “smart” products like “intelligent” clothes, household appliances, fitness equipment, toys, personal assistants, learning devices, etc., our whole lifeworld becomes more and more embedded in a fine-grained network of sensors able to monitor and register everything we say or do.<sup>12</sup> For the sake of shiny things as convenience, optimization, and “enhanced user experiences,” we are piece by piece trading away the former virgin territory of our intimate social life. Device by device, we are building our own privately run, commercial Panopticon with no space left for privacy. Neither will it be possible to *opt out* even if it is not mandatory and no one forces one to buy anything. Already today, the Internet is deeply embedded in our societies and our social, communicative, economic, and politically infrastructure. Getting an education, finding employment and securing an income, having a credit card and a bank account, participating politically, ad communicating and interacting socially without being a part of the digital infrastructure is uphill to say at least. With the development of the Internet of Things and “smart cities,” going into the wilds may be the only alternative to total surveillance—which is no real alternative at all.

---

<sup>11</sup>Google CEO On Privacy (VIDEO): ‘If You Have Something You Don’t Want Anyone To Know, Maybe You Shouldn’t Be Doing It’, *Huffington Post*, 18.0.2018. Verified 24.06.2018: [https://www.huffingtonpost.com/2009/12/07/google-ceo-on-privacy-if\\_n\\_383105.html](https://www.huffingtonpost.com/2009/12/07/google-ceo-on-privacy-if_n_383105.html)

<sup>12</sup>See Chap. 1, Sect. 1.7.

Google is one of many. The business model based on data mining, Google pioneered, has become a standard business model and yardstick for new startup companies, providing a service, some entertainment, a utility, or information in exchange for user data. There is a data fever going on comparable to gold rushes of the nineteenth century.<sup>13</sup> With a lot of different actors racing for getting a piece of the new action—and as the data assets are mined and appropriated at this new frontier of commercialism and commodification—we are dispossessed of the information our behavior produces. We are alienated from the value our data creates and lose control. Data enables prediction and prediction makes for control. The data we are providing is used to control us.

## 7.4 Prediction is Profit

The main reason data is valuable when pooled and aggregated into Big Data is that it enables predictions of the future. Data provides patterns of past behavior that may show probable future behavior. It makes possible data-informed calculations of risk, future sales, gains and expenses, effects of marketing, and communication strategies as well as on how to optimize communication, marketing, and design. If you are able to calculate probable future behavior, you are able to make a profit from it:

Will she be able to repay the loan in the future – and will she? Will he show up for work and contribute to productivity or is he just a “high cost” employee? Is she disposed for a disease, so the insurance company in case a policy is made has to cover medical expenses exceeding the income from premiums? Which commercials will succeed persuading this person to buy the product or vote for the candidate? How many more users will push the button and provide valuable attention, if it is red? Which products and services will he desire later today? In two minutes? Ten seconds after this specific online marketing stimulus is provided through his smartphone?

---

<sup>13</sup>Jankowski, S. (2014). The Sectors Where the Internet of Things Really Matters, *Harvard Business Review*, 22.09.2014. Verified 24.06.2018: <https://hbr.org/2014/10/the-sectors-where-the-internet-of-things-really-matters>

All these questions come down to the same: how may future profits be generated and maximized? Data-driven prediction of behavior for the sake of sales and profit is the essence of the leading surveillance capitalism business model.<sup>14</sup> Fortune telling has become big business. Prediction is profit.

Profitable predictions may become chains restraining and undermining the self-determination of the citizen. In a free data market unrestrained by effective citizen protection laws, the traditional *financial* credit rating scores may start to look like the all-embracing *social* credit scores in China.

With Big Data extraction and analyses, the market for consumer and credit information in the USA has become the Wild West. The traditional credit bureaus formerly operating in regulated territory have transformed into data brokers with the will and ability to circumvent the law—at the expense of citizens’ rights. Whereas individual level information is regulated by law, the information it is possible to extract through data mining is not. With sufficient data, it’s possible to calculate information just as sensitive as individual level information. An event title in 2011 by two of former American credit bureaus turned data brokers, FICO and Equifax, is telling: “Enhancing Your Marketing Effectiveness and Decisions With Non-Regulated Data.”<sup>15</sup> In the new unregulated domain of data-driven credit scores, the approach is that “all data is credit data.”<sup>16</sup> With such an *anything-goes* approach, profile data, and online social footprints, the device you use and how quickly you scroll through the sites are nowadays factors that may feed into your credit score. Facebook has taken it further

---

<sup>14</sup>Zuboff, S. (2016). “The Secrets of Surveillance Capitalism,” *FAZ*, 05.03.2016. Verified 24.06.2018: [http://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshana-zuboff-secrets-of-surveillance-capitalism-14103616.html?printPagedArticle=true#pageIndex\\_0](http://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshana-zuboff-secrets-of-surveillance-capitalism-14103616.html?printPagedArticle=true#pageIndex_0)

<sup>15</sup>Taylor, A. & Sadowski, J. (2015). “How Companies Turn Your Facebook Activity Into a Credit Score,” *The Nation*, 27.05.2017. Verified 24.06.2018: <https://www.thenation.com/article/how-companies-turn-your-facebook-activity-credit-score/>

<sup>16</sup>Lauer, J. (2017). *Creditworthy: A History of Consumer Surveillance and Financial Identity in America*. New York: Columbia University Press: 267.

and has patented a method to calculate credit scores based on one's social network, so the average credit score of one's friends is decisive for one's own (Hurley and Adebayo 2017). In a capitalist country as the USA, access to credit is a make-or-break for everyone but those in the top 1% of the wealth and income scale. To buy a house, you need a mortgage; you need a loan for buying a car and getting a college degree for yourself or your children depend on access to credit and student loans. Employers also consider credit rating scores when hiring and so do property owners evaluating potential tenants. With no effective legal restrictions on gathering and usage of data, the door is open for insurance companies gathering data on health and habits undermining the whole idea of pooling risk in insurance products and making it impossible to get insured for the ones most in need. Your credit rating score is decisive for the opportunities you have and the restrictions you face. If there is no limit to what goes into one's credit score and how it is used by creditors and banks, landlords and car rental companies, and employers and insurance companies, the difference between financial credit rating and *social* credit rating in China is diminishing.

## 7.5 Prediction Is Power

Prediction is power. If you are able to predict the future, you may also be able to influence and change it—and make a buck doing so. Predict to change is the core of targeted marketing. Marketing success is success in changing people's behavior in a commercially or politically profitable way for the client. To be able to predict behavior makes it possible to change and modify it by providing the right stimuli at the right moment. If you can predict what people want and when they want it, it is possible to precision nudge and steer them to buy it from you. The more you know, the better you are able to predict, and the better you predict, the more successfully you may influence and control. Already demographic profiling grants this kind of power. Predictions made from data such as home address, gender, ethnicity, employment,

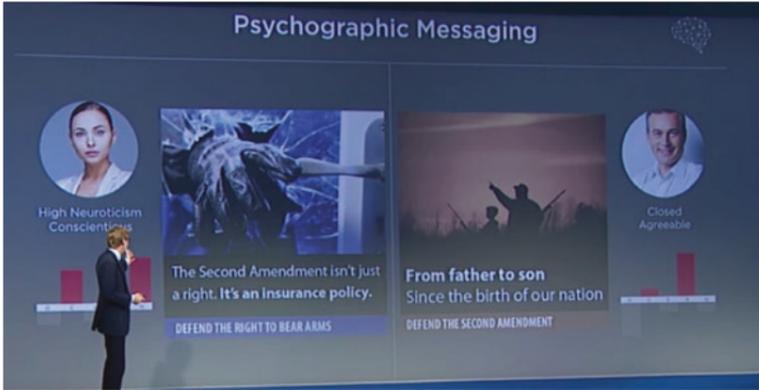


FIG. 7.3. Former CEO of *Cambridge Analytica*, Alexander Nix, illustrates the potential in psychological profiling. The right to carry arms is the message to be sold, and if you are the fearful type (high score on neuroticism), the ad will play on fear of burglary and the right to carry arms is framed as an “insurance policy” (left). If, however, you are profiled as “closed” or tradition-bound, but “good-natured,” the political marketing is tailored to *this* profile and the right to carry arms is framed with a hunting metaphor, patriotism, and family values: “From father to son. Since our nation was born” (right). (Wozniak, K. (2017): “Did Big Data Win the Election for Trump?,” *Misciwriters*, April 18, 2017. Verified June 14, 2017: <https://misciwriters.com/2017/04/18/did-big-data-win-the-election-for-trump/>).

income, consumption patterns, political affiliations, and social network of family and friends make it possible to target and tailor ads to hit the pain points where it hurts. An effective predatory method for influencing people’s behavior.<sup>17</sup> However, when the profiling moves under the skin and becomes psychological profiles of people’s mental makeup and emotional life, it gets even more powerful and potentially oppressive.

Before the scandal, Cambridge Analytica also boasted that they are taking things a step further with profiling, integrating methods and results from scientific psychological research to

<sup>17</sup> See Chap. 1, Sect. 1.8.

create *psychological* profiles of users/consumers/voters/citizens. If you can categorize people according to their personality type and mental makeup, the targeted marketing bombardment may be conducted with even more precision and effect. Psychological profiling opens up chilling possibilities of affective management and emotional control. By employing, for instance, fear-mongering messages for someone profiled as a fearful personality type, it is possible to hit the target's pain points where it *really* hurts (Fig. 7.3).

Even if Cambridge Analytica was the one scandalized company that got caught, it is not alone with ambitions of affective influence and emotional control made possible by psychological profiling. It is highly potent, according to Alexander Polonsky, from the French data broker company Bloom:

You can do things that you would not have dreamt of before. It goes beyond sharing information. It's sharing the thinking and the feeling behind this information, and that's extremely powerful.<sup>18</sup>

Powerful for *whom*, one might ask. Not the user, costumer, or citizen who is psychologically profiled to be effectively influenced and manipulated. The dream of a data broker may turn to a nightmare for the citizens. The scare of *The Hidden Persuaders* (Packard 1960) steering us secretly through subliminal influences in the 1960s may turn out to be fully justified in the age of Big Data and psychographics. Psychological profiling takes the knowledge that is power to the next level. Most of our life and behavior is governed by fast, automatic, involuntary, and unconscious mental processes evading our attention and awareness (Kahneman 2011). Humans are affective beings, rather than rational agents, and more controlled by emotions than we are in control of them (Haidt 2012). If you are able to influence those processes and associations, affects, and emotions going on in the dark basement

---

<sup>18</sup>Confessore, N. & Hakim, D. (2017). "Data Firm Says 'Secret Sauce' Aided Trump; Many Scoff"; *New York Times*, 06.03.2017. Verified 07.01.2018: <https://www.nytimes.com/2017/03/06/us/politics/cambridge-analytica.html>

of our *psyche*, you can more or less control us. If one is taking advantage of people's deepest fear, makes them angry, or otherwise plays emotionally on fundamental personality traits, we may not even be aware of, it may undermine individual self-determination, rational agency, and autonomy. If companies—or the state for that matter—know us better than we know ourselves, an “emotional dictatorship” governing us without our knowledge or consent is right down the road. As conceived by the South Korean-born German philosopher and writer Byung-Chul Han:

“Big Data” enables prediction of human responses and the future, therefore, can be manipulated accordingly. Big Data has the ability to turn people into puppets. Big Data generates knowledge that enables ruling power. And it is Big Data that makes it possible to access and manipulate the human psyche without the affected person being aware of it. Big Data essentially spells the end of free will.<sup>19</sup>

If this extreme situation of a data-driven total elimination of free will, individual sovereignty, and autonomy is ever fully reached, it would be the opposite of emancipation. Total predictability makes for total control. Freedom from uncertainty is not freedom at all. On the contrary, it is the stuff totalitarianism is made of.

## 7.6 Roads to Totalitarianism

According to Hannah Arendt, the aim of totalitarianism is total, unlimited power. This kind of power demands that everybody is “dominated in every aspect of their life” (Arendt 1951: 456). The greatest obstacle to that ambition is the unpredictability of humans due to our spontaneity, creativity, and freedom. Those must be eliminated to produce predictable subjects and humans reduced to bundles of conditioned reflexes controllable by stimuli to provide the desired

---

<sup>19</sup>Han, B.-C. (2016). “Digital Totalitarianism: How Big Data Is Killing Free Will”, WorldCrunch, 07.05.2016, verified 26.06.2018: <https://www.worldcrunch.com/culture-society/digital-totalitarianism-how-big-data-is-killing-free-will>

and predicted response. Thus, the aim of totalitarianism is identical to a real-world actualization of behaviorism's deterministic understanding of human beings: stimuli-response. With the pace and acceleration, new digital technology is developed and integrated with behavioral science and design, and we may be heading toward—but hopefully never reach—a digital totalitarianism: *the total elimination of autonomy and self-determination by data-driven behavioral control*.

Long before the digital revolution, Arendt worried that the historical tendency is not leading us toward emancipation and a realization of freedom, but to the opposite:

The trouble with modern theories of behaviorism is not that they are wrong but that they could become true, that they actually are the best possible conceptualization of certain obvious trends in modern society. It is quite conceivable that the modern age — which began with such an unprecedented and promising outburst of human activity — may end in the deadliest, most sterile passivity history has ever known. (Arendt 1951: 345)

With the brave new digital world and the marketization of user data, this worry has not become less pertinent.

Traditionally, totalitarianism is identified with *state* totalitarianism and characterized by the abolishment of any distinction between the state and civil society. Nothing outside and exempted the total dominion of the state.<sup>20</sup> The “total state,” according to its advocate, Carl Schmidt, “embraces every domain” with the result that everything is “potentially political” (Schmidt 1932: 22). It is *the total interpenetration of the political and social and of state and society*.

It does not take a *state* with totalitarian ambitions to reach totalitarian results. The ambition of total monitoring and modification of our life and behavior is the ambition of *big business* in the tech industry: to appropriate, colonize, commodify, and monetize every last piece of our life and behavior for the sake of profits. As a Silicon Valley developer of learning applications states the corporate mission:

---

<sup>20</sup>Mussolini, B. (1932). *The Doctrine of Fascism*. Verified 24.06.2018: <http://www.worldfuturefund.org/wffmaster/Reading/Germany/mussolini.htm>

The goal of everything we do is to change people's actual behavior at scale. When people use our app, we can capture their behavior, identify good and bad behaviors, and develop ways to reward the good and punish the bad. We can test how actionable our cues are for them and how profitable for us.<sup>21</sup>

Regulating behavior in real-time employing gamification and incentives of rewards and punishments as means is a mission shared by the Chinese State Council and Silicon Valley operatives. In China, for the sake of “trustworthy,” conformity to norms, social order, and harmony—in Silicon Valley, for the profits. Without regulation, restrictions, and citizen protection in the data economy, a new variant of *Corporate Totalitarianism* may manifest.

Corporate totalitarianism may be defined as the total interpenetration of the social and the *profitable* and the identification of *market* and society. Everything is potentially profitable. There is no value outside of the market—no value but market value. If all aspects of our life are marketized and commodified as raw material for generating profits, the market and the commercial domain of commodities has become all-embracing with nothing existing or having value outside. Quite contrary to libertarians as Rand and Ron Paul's identification of less market regulation with increased individual freedom and self-determination,<sup>22</sup> this sort of market fundamentalism actualized in the age of Big Data may yield totalitarian results. From a citizen perspective, a multiplicity of different actors competing internally in an unregulated market of data and information may result in an information regime not radically different from the centralistic Chinese system. If everything one does is seen, registered, evaluated,

---

<sup>21</sup> Zuboff, S. (2016). “The Secrets of Surveillance Capitalism,” *Frankfurter Allgemeine Zeitung* March 5th 2016. Verified January 11th 2017: <http://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshana-zuboff-secrets-of-surveillance-capitalism-14103616.html?printPage&Article=true>

<sup>22</sup> The Technology Revolution: A Campaign for Liberty Manifesto. Verified 24.06.2018: <https://www.scribd.com/doc/99220534/The-Technology-Revolution>

and get rewarded or sanctioned accordingly, the result is a perverted proxy of an omniscient God judging and making sure everybody *reap as they sow*. *The Big Other* may be at least as powerful and oppressive as Big Brother:

[The Big Other] is a ubiquitous networked institutional regime that records, modifies, and commodifies everyday experience from toasters to bodies, communication to thought, all with a view to establishing new pathways to monetization and profit. Big Other is the sovereign power of a near future that annihilates the freedom achieved by the rule of law. (Zuboff 2015: 81).

Technological progress is not necessarily progress for humanity—it may be the opposite. “Free stuff” online may just turn out to be extremely expensive, especially if one is not aware of the full price. It may cost us our democracy, our self-determination, and in the end our freedom.

**Open Access** This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter’s Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter’s Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

