2 Surveillance fiction and transparent society

"The future's already here: It's just not evenly distributed."
William Gibson (1999)

2.1 A new surveillance sensibility

Practices of strategic observation, monitoring and data gathering have been a topic of public concern throughout the 20th century and have been explored by authors of fiction in many ways. Yet, compared to the 1940s and -50s with their Cold War espionage sensibility, or the wave of conspiracy and paranoia narratives of the 1960s and -70s, the current cultural climate and the narrative registers that accompany it are again different. Since the 1980s and the end of the Cold War, a new kind of sensibility towards centralised, bureaucratic surveillance by states and corporations has formed in response to the increasing importance of digital technologies such as databases[8] and digital networks. While the spectre of the 'surveillance state' was at the centre of public debates in the 1980s, authors of the science fiction subgenre Cyberpunk have begun to investigate the economic impact of digital networks from a transnational perspective since the early 1980s. The large-scale introduction of video camera networks in British and US cities during the 1990s have provoked another set of, often heated, public debates. With the normalisation

[8] The protests in Germany that led to the so-called "Volkszählungsurteil" (1983) of the German Constitutional Court were inspired to a large degree by the fear of a digital national population database and the future uses to which it could be put.

of video surveillance systems as a regular policing infrastructure CCTV has become a common theme in fiction.

Since 2001, another set of concerns has provoked intense debates about surveillance: The post-9/11 security state took shape and received sweeping powers in the field of communication surveillance and the detention of terror suspects. While already marginalised social groups like Muslims were targeted now with doubled intensity by the security apparatus, the new legislation also curtailed the legal protection hitherto granted to journalists and lawyers who want to protect anonymous sources. Moreover, the theme of the surveillance state continued to create unease and resistance in the mid to late 2000s (2004–2010) in Britain when Labour governments tried to introduce national ID cards and a central digital register of the population. Due to large protests and a change of government in 2010, the new Conservative-Liberal government buried the ID card scheme.

Central for the present study are the developments since the early 2000s when the social impact of the internet and its new economy became increasingly tangible, leading to intense debates about the character and outcome of the so-called digital revolution. But while most commentators in these early debates were busy discussing the internet in black and white terms as either utopia or dystopia, these debates missed the man-made, material character and the increasing political dimension of the internet's architecture. "Meanwhile", as Marianne Franklin points out in her instructive study *Digital Dilemmas: Power, Resistance and the Internet* (2013), "the internet, and the cyberspaces it facilitates, has been bought and sold several times over by increasingly powerful corporate agglomerations" (2013, 182). The free-market approach to media regulation favoured by governments since the 1980s provided venture-capital-backed internet start-ups with the chance to claim large amounts of online territory and shape it according to their interest. This resulted in a relatively small number of globally dominant companies exerting overwhelming power over the digital economy today by controlling the user-facing architecture and underlying platforms. Within two decades of its going public in 1994, this socio-economic dynamic led to a transformation of the decentralised, open and public architecture of the internet into the now familiar landscape of dominant,

advertising-finance web services based on dataveillance and owned by a small number of monopolistic, highly profitable software platforms. As a result, the IT-policies of companies like Google and Facebook have an overwhelming influence on the shape of the internet as an economic arena and socio-cultural space.

Besides the traditional business models of selling soft- and hardware, a new kind of data-driven business model has emerged which is based on the, mostly clandestine tracking of user communication and behaviour. As pointed out above, this shift is indicative of an emerging economic model that can be described as "surveillance capitalism" (cf. Zuboff 2015, 75). Other terms like 'data-point economy'[9], 'data capitalism' and 'information capitalism' are also used in critical discussions about business models of digital tracking and data mining. Despite differences in terminology, critical scholars describe the status quo in roughly similar terms. Internet pioneer and Silicon Valley critic Jaron Lanier makes the following point in his political essay *Who Owns the Future* (2014):

> There is no definitive map of network spying services. The allegiances and roles are multifarious and complex. No one really knows the score, though a common opinion is that Google has historically been at the top of the heap for collecting spy data about you on the open internet, while Facebook has mastered a way to corral people under an exclusive microscope. That said, other companies you've probably never heard of, like Acxiom or eBureau, are also deeply determined to create dossiers on you. Because spying is, for the moment, the official primary business of the information economy. (2014, 100)

Around the personalised data-driven advertising systems of Google and Facebook, a transnational data brokerage industry has emerged that collects and shares personal information about individuals and

[9] A term used by the organisers in 2015 at *Transmediale Art and Digital Culture Festival* at Haus der Kulturen der Welt, Berlin.

social groups for commercial purposes. These increasingly automated processes of data collection, sharing, categorisation and scoring of individuals undermine established legal data protection and privacy regimes and expose populations to a number of risks. In particular, forms of social discrimination and exclusion, as a result of "social sorting" practices (cf. Lyon 2003), are discussed by scholars and legal practitioners. This risk results from the widespread use of Google's and Facebook's seemingly cost-free online infrastructures which now perform vital communicative functions for societies. Moreover, the business model of dataveillance-driven online marketing also poses a significant risk for manipulation of the digital public sphere as the elections of the past years have shown. This theme will be taken up in the discussion of Dave Eggers's *The Circle*.

While researchers have to adhere to high ethical standards when gathering, collating, analysing and sharing sets of information about individuals collected as part of their work, there do not exist sufficient legal and ethical norms for the commercial dataveillance practices of contemporary data capitalism. The fact that most of these activities are legally covered by take-or-leave terms of service and protected by intergovernmental agreements[10] does not change this assessment. The large majority of citizens is unaware of the extent to which their communication and behaviour is observed and analysed[11] online. Certainly, a basic understanding of the existence of dataveillance has

---

[10] Prior to the EUs General Data Protection directive (2018), the "Privacy Shield" agreement (2016) between the EU and the US and its precursor "Safe Harbour" (2000–2016) were designed to exempt the wide-ranging practices of data collection and analysis of US companies from EU data protection law. This self-regulation approach also gave US companies a competitive advantage over European competitors.

[11] Max Schrems, the Austrian law student who challenged Facebook successfully in October 2015, achieved a watershed ruling by the European Court of Justice (EJC) which declared the "Safe Harbour"-agreement between the EU and the US unlawful. Schrems received a DVD from Facebook with all the information permanently stored about his user activities on Facebook. On his website, he lists the more than

emerged during the last decade, yet the black box character of this new industry prevents the emergence of a clear understanding among citizens. A representative study from Germany by media psychologist Sabine Trepte shows that a majority of citizens is concerned about the dataveillance practices of internet companies, but feels it has no choice to avoid it (cf. Trepte, Masur 2015). Trepte and Masur oppose the notion that the widespread usage of these dataveillance-financed online services is based on informed consent. Instead, the discrepancy between the anxiety of commercial dataveillance on the one hand and the usage of these services on the other, which is discussed as the 'privacy paradox' among researchers, is also largely the result of disillusionment and the impression that there is no alternative to signing away one's decision rights over personal information in exchange for using such services, the study by Trepte and Masur suggests. Two thirds of the respondents said that they see no other chance if they want to use these services (cf. 2015, 8).

Three years before the Snowden leaks, Cultural Studies scholar Claire Birchall already stressed that the majority of citizens today occupies a shared, inferior position as data subject in relation to the new security state. Stripped of agency over the interpretation and use of information inferred from surveillance data, Birchall describes the implications of this for political subjectivity as the production of a transnational "datatariat" (2011, 43). It consists of those who are "encouraged to make use of and be used as data; a mass connected through data access, production, accumulation, and exploitation" (2011, 43.). With regard to dataveillance practice of contemporary information capitalism, the subject can be said to be in a similarly inferior position. As I will show in my discussion of Eggers's *The Circle,* digital tracking online is not limited any longer to the use of Google and Facebook services, but increasingly happens across the internet and the digital devices available to consumers.

From the above said, three interrelated aspects can be made out to have a direct bearing on the increasing sensibility for surveillance

---

50 categories of personal information the Facebook documentation contained about him (cf. Schrems 2015).

this study traces in contemporary fiction: first, the technological transformations discussed under such diverse labels as 'data mining', 'big data analysis' and 'dataveillance'; secondly, the economic processes connected to the new, transnational information and data capitalism; and thirdly, the rise of the digital information and security state. These interrelated developments cause considerable unease today. A growing cultural awareness of these trajectories, I argue, informs the new surveillance sensibility. This rising sensibility regarding questions of power over data and information derived from it in digital networks is often paralleled by unease that shows, for example, in tropes such as the uncanny idea of "data doppelganger" used in debates about commercial data-mining (cf. Watson 2015).

It is indeed not only the new data capitalism that shapes the contemporary socio-technical landscape. The state also draws on and shapes the form of digital technologies as well as the norms that regulate their application. Franklin even sees a "return of the state", after many years of neglecting the internet which gave

> [...] commercial interests a free hand in cornering the market in research and development of the internet's strategic resources, web-based news and entertainment, provision of public services and their accompanying digitalization. (2013, 183)

Besides these two groups of powerful actors – transnational corporations and governments –, parliaments, public institutions, non-governmental organisations and other civil society actors played and continue to play a role, too, in the development of the internet and its adjacent technologies. This impact includes both the development of the internet's original infrastructure and that of open software – from operating systems (Linux) to browser and communication technologies (Firefox, E-Mail clients, etc.) and Office software. The efforts of transnational communities to develop, for example, open software as a public good and to foster its distribution, the influence of information technology and scholarly communities as well as the voices of open culture, creative commons and digital rights activists, increasingly also from post-colonial settings, will continue to play a considerable role in the way the internet is

governed, as Franklin argues (cf. 2013, 31). Although the power of states and corporations is comparably higher, considerable amounts and forms of agency are located within these communities of practice due to their technological, legal and political expertise and effective forms of organisation and communication.

The power struggles around the design of the internet and the future of the digital revolution also include intense efforts by all actors to "control the narrative" (Franklin 2013, 2) around the digitalisation of society:

> Each perspective [corporations and advocates of an open, socially inclusive internet] denotes a particular ethos about freedom, regulation, and openness, and each in turn represents a different view of the internet's future. Both camps, and the various players who shuffle between the two (national and local governments in particular), stake a claim in narratives of which approach governed the internet's past. This longstanding standoff behind the screen, indeed at the user-interface itself, casts another light on the link between the ordinariness of the internet and the high-level struggles over its governance and corporate and state-level exertions to extend or maintain direct ownership if not regulatory control of internet design, access and use. (2013, 29)

Taking all this into account, the familiar notion of technology as neutral must be qualified. The form and character of technology is profoundly embedded in the social, because technologies are always developed and applied for specific social uses, as Raymond Williams explains (cf. 2003, 7). These social uses and interests can be commercial or non-commercial, repressive or non-repressive, characterised by a spirit of social in- or exclusion. However, they are never neutral.

2.2 The impact of the Snowden leaks

The Snowden leaks in 2013 constituted a major watershed for public discussions about state surveillance and the formation of the contemporary critical surveillance sensibility comparable, in cultural terms, only to the Watergate scandal.[12] The revelations about US-led online-surveillance and the heated discussions around the disclosure of the documents had a decisive influence on this study as they highlighted the relevance of the body of fiction under examination here. Although the debates triggered by the documents revealed through whistle blower Edward Snowden had no influence on the production of the fictional works discussed in this study[13] the leaked documents are nevertheless important as they confirm much of the hitherto vague picture of the so-called "Total Information Awareness" (later "Terrorist Information Awareness") programme introduced by the US government after 9/11. This initiative and the legislation that enabled it, namely the US Patriot Act 2001, formed the basis for the mass surveillance activities of US security services and their international partners. As a result, the US Department of Homeland Security was created in 2002, and a trend towards the militarisation of policing in the US began. These developments form the background for Cory Doctorow's young adult novels *Little Brother* (2008) and *Homeland* (2013). The Snowden leaks also provoked reactions from numerous authors, film-makers, artists and intellectuals. The German authors Julie Zeh and Ilja Trojanow, for example, initiated an international campaign under the title "Writers against mass surveillance" with an open letter that was signed by hundreds of authors and published in newspapers worldwide.

The public debate about the Snowden leaks developed very differently in Britain and the US. While the discussion in the US was carried by a broad alliance of media outlets and parliamentarians and led, as a result, to changes in the regulation of secret services, the

---

[12] A full overview of the revelations cannot be given here. For a concise introduction: cf. Greenwald 2014.

[13] All three novels have been published before the event.

British discussion was stifled by the fact that most newspapers and politicians in the opposition sided with the government that threatened the newspaper legally. The *Guardian* newspaper, whose role as an independent, transnational media outlet had been decisive for the publication of the material collected by Snowden, remained alone with its reporting on the Snowden leaks. This is astonishing, given the amount of resistance raised against the spectre of the digital Big Brother state in Britain between 2004 and 2010 when Labour governments began, unsuccessfully, to introduce an ID card backed by a central register.

Only few British authors raised their voice in defence of Snowden and the *Guardian*. When the newspaper offered literary author and journalist John Lanchester access to the documents collected by Snowden, he was hesitant at first, too. He was not convinced that the material contained information the British public needed to know. As the British government had forced the *Guardian* to destroy its digital copies of the material in London, Lanchester flew to New York to study the material. Having done so, he changed his mind and wrote a long essay for the *Guardian* entitled "The Snowden files: why the British public should be worried about GCHQ" (2013). It is one of the most precise and accessible analyses of the Snowden material published so far.

His report of the Snowden files is a warning to the British public that the country is "on the verge of being an entirely new kind of human society, one involving an unprecedented penetration by the state into areas which have always been regarded as private" (cf. ibid.). British society, Lanchester argues, is too complacent when it believes that police states could only exist elsewhere. A police state "isn't a country where the police strut around in jackboots; it's a country where the police can do anything they like." It is exactly such a mentality and ambition "that the security establishment can do anything it likes", which Lanchester like Glen Greenwald[14] has spotted in the Snowden files.

---

[14] The US journalist and lawyer who received the first copy of the leaked material and subsequently published articles from it (cf. Greenwald 2014).

Lanchester finishes his essay by proposing two steps for political reform: The inclusion of public representatives into the 'secret circle' of judges who decide over the legitimacy of targeted as well as mass surveillance operations; and the introduction of a digital bill of rights:

> Digital surveillance must meet the same degree of explicit targeting as that used in interception of mail and landlines. [...] There can be no default assumption that the state is allowed access to our digital life. (Lanchester 2013)

What Lanchester doesn't address is the breadth and depth of the state-private system established by governments during the last decades. In the US, as the Snowden documents show, secret services and other state agencies have been given unchecked powers to access the servers of internet companies and telecommunication providers enabling them to analyse a historically unprecedented amount of personal information of its citizenry (cf. Greenwald 2014, 109ff).

John Lanchester has also addressed the post 9/11 security culture in his fiction. In his novel *Capital* (2012), written and published before the Snowden leaks, Lanchester had already explored various forms of surveillance, including interpersonal surveillance as well as state dataveillance. One of the protagonists of *Capital,* Shahid, a Muslim from London, agrees to give shelter to an old friend who has radicalised since they have last met. Shortly after his friend moves out, Shahid's IP-address is found to have been used for communication in relation to a bombing plan of an Islamist group. As a result, Shahid is mistakenly arrested and held in custody under anti-terror law under the allegation that he is responsible for the communication made from his computer. Although the police cannot prove that Shahid contributed to the bombing plot, they detain him at a place unknown to him or his family without access to a lawyer or contact to his family. In order to increase the pressure, the police make use of the full 28 days of prison without charges which are at their disposal on the basis of the UK Terrorism Act 2006. Taken from his house by the police in a night raid and stripped of his citizen rights, Shahid feels as if detained by an authoritarian regime.

One of the novel's strongest moments is the portrayal of Shahid's experience in prison. It illustrates the fundamental erosion of trust in the police and the state which subjects thus detained might experience. Yet, *Capital* also includes a sense of hope in democratic procedures as Shahid's family is able to get in contact with an experienced lawyer. The civil rights lawyer finally manages to find out where Shahid is held and can achieve his release. Yet, Shahid's social reputation and his trust in British society may be irreversibly damaged, resulting ironically in the danger of him seeking recognition by radical Islamist groups the novel might be seen to imply. Lanchester's novel thereby draws attention to the psycho-social effects of the heightened degree of the new security state's surveillance apparatus to Muslim communities since 9/11 and the London bombings of 7 July 2005. In the Kafkaesque world of digital mass surveillance which seeks to monitor populations from a distance, such cultural effects are largely invisible to the wider public. This problem is heightened by uncertainty about how long surveillance data is being stored and to whom it is being made available.

Even to many IT professionals and those who have researched surveillance technologies since the end of the Cold War – from activists to artists and researchers –, the scale and scalability of the new global surveillance system exposed by Edward Snowden were unexpected. The fact that the system relies heavily on the information about citizens collected by the private sector, in particular the leading, US-based IT companies, draws attention to a deeper cultural dynamic that drives this state-private partnership: What became fully apparent through the Snowden documents is not only the extremity of the US and UK governments' position on what might be called social transparency – captured in the title of the above mentioned "Total information awareness" programme –, but also the risks associated with the commercial dataveillance carried out by global corporations like Google and Facebook.

The rise of the current surveillance sensibility which this study traces through works of fiction published between 2003 and 2013 is closely connected to these issues and the struggles around the politics of digital and networked technologies since the early 1990s. The iconic surveillance cameras, debates about which dominated

the 1990s, may seem somewhat outdated in comparison to the internet and without relation to it, but on a deeper socio-techno level, CCTV camera networks with their ever-increasing technological sophistication are part of the underlying cultural logic of making legible the social for governmental and commercial reasons.

2.3 Investigating the intersection of society and technology

Fiction is, of course, more than a set of cultural documents we can study for symptoms of changing cultural sensibilities and anxieties. Beyond their cultural-historical dimension, works of fiction possess a cultural agency of their own. Like academic researchers, authors of fiction observe the social and produce cultural knowledge in the form of fictional discourse. It is in this dialectical sense that fiction simultaneously articulates a growing cultural surveillance sensibility and at the same time shapes it. Authors who engage with the problems of digital surveillance create narrative mappings of the socio-technical present and thereby produce knowledge. Yet, unlike academic or journalistic discourse, fiction dramatises and narrativises its material in order to let events and the actions of characters speak. Building narrative models of the social through the representational apparatus of literature, film, theatre and the specific genre traditions that have evolved during modernity, authors of fiction engage in a communicative contract with their readers that fundamentally differs from non-fictional discourse, as described in the previous chapter. Fiction, and with regard to this study: surveillance fiction, I argue, constitutes a form of philosophy or research about Culture and Society that needs to be studied according to its own terms of production and reception.

Like in journalistic and academic discourse about surveillance we find various philosophies, or ideologies, within fictional discourse, too. While some of the works discussed in this study focus in sociological terms on the impact of surveillance cameras on everyday life in local contexts others map how the current economic system produces specific forms of control through dataveillance, for example

in shopping centres or at the workplace, in retail or in management. Some works focus on the ethics of watching and the risk of abuse that comes with surveillance power, while others explore the psychic life of the subject under surveillance. Aesthetic traditions, styles and genre families play a decisive role in the ways in which authors investigate surveillance practices and the social in fiction because these have evolved narrative means to explore and represent the phenomena that authors seek to address. More will be said about this in the fourth and fifth chapter of this study.

William Gibson is one of the leading literary voices to explore the impact of digital technology on the social. Since he publicised the Cyberpunk novel *Neuromancer* (1984), he has published numerous novels and essays about the politics of the digital. In an essay published in the *New York Times* in 2003 entitled "The Road to Oceania", he gives an accessible introduction to the philosophy of digital technology that underlies his fiction. In the text, Gibson argues that Orwell's *Nineteen Eighty-Four* (1949) was not a prediction but a description of Britain in 1948, albeit encoded in terms of science fiction. It should therefore not be used as a model to describe today's networked media system and digital information state, he explains. Characterised by a broadcasting paradigm, the surveillance system in Orwell's anti-utopia neither resembles nor intendeds to project the socio-technical status quo of the year 1984, let alone that of the early 2000s, Gibson insists (cf. 2012, 168).

Although I don't fully agree with this in media-theoretical terms, because Orwell's telescreen-system has a back channel and thus extends the broadcast model towards a more cybernetic model, Gibson's point is instructive. The surveillance regime in Oceania is neither a peer-to-peer-network nor a platform but a centralised form of a network used for the broadcasting of propaganda and the centralised observation of citizens. Such a star topology model that contains a strategic centre was very prominent in early cybernetics debates of the 1940s and 1950s.[15] This positions Orwell at the beginning of the cybernetic age.

---

[15] Cf. Norbert Wiener's *Cybernetics or Control and Communication in the Animal and the Machine* (1948).

Gibson makes another helpful point in this essay when he highlights that local, closed systems of data collection and surveillance increasingly tend towards integration within larger information sharing architectures due to the digital transformation:

> Today, on Henrietta Street, one sees the rectangular housings of closed-circuit television cameras [...] the street seeming itself to have evolved sensory apparatus in the service of some *meta-project* beyond any imagining of the closed-circuit system's designers. (2012, 67f; italics added)

What is this "meta-project" Gibson alludes to in this quote? He immediately answers this question himself: "[...] we are approaching a state of absolute informational transparency" (2012, 168). The meta-project Gibson introduces here is the idea of a digitally transparent society which he regards as an unwanted, though unavoidable by-product of the development of digital network technologies (cf. 2012, 168f). He points to an underlying socio-technical dynamic of increasing information mobility that is inherent in digital technology in its current form:

> That our own biggish brothers, in the name of national security, draw from ever wider and increasingly transparent fields of data may disturb us, but this is something that corporations, non-governmental organizations and individuals do as well with greater and greater frequency. The collection and management of information, at every level, is exponentially empowered by the global nature of the system itself, a system unfettered by national boundaries or, increasingly, government control. (2012, 169f)

2.4 Social transparency as surveillance

15 years into the future, this conclusion still sounds right. Yet, Gibson's essay from 2003 carries strong undertones of technological determinism that he might himself object to today. These were part of the