Surveillance and the Impossible Search for Ideal Behaviour

Toine Spapens

Abstract Information and communication technology and the internet created unprecedented opportunities for collecting “big data” and apply it to surveillance and influence the behaviour of citizens, for instance in their roles of voters, customers, partners and workers. There is a growing risk that data on these different roles is exchanged and combined for which it was not collected. Surveillance may be defended from the perspective of law and order, protection of safety and health, and economic development, but it may also impact negatively on several United Nations (UN) Sustainable Development Goals (SDGs) to be attained by 2030. Being one of the crucial issues in the world today, it comes as no surprise that the topic is being studied by lawyers, urbanists, sociologists, computer scientists, political scientists and others. However, criminologists have until now mainly looked at surveillance in the context of preventing and detecting crime and terrorism from a “what happens and what works” angle. This chapter will apply a broad perspective by taking the social construction of deviance as a starting point and addressing the consequences of the definition for those who do not live up to the ideal, in terms of criminalisation, social exclusion and other potential effects, keeping in mind the context of the UN’s development goals.

Keywords Big data · Mass surveillance · Social construction · Sustainable development goals · Crime prevention · Risks

1 Introduction

Today, we undoubtedly live in an era of mass surveillance, defined as the ability of State and private actors to monitor citizens’ and customers’ whereabouts, interests and behaviour. In this chapter, I will address this development from a criminological
perspective. State actors foremost legitimise the gathering of such information by the fact that it helps to solve and prevent crimes, and terrorism in particular, and more recently since the COVID-19 crisis, to reduce the risk of infection. Dictators may use surveillance as an instrument to stay in power. Commercial operators primarily legitimise the gathering of customer data by stating that it helps them to improve their products and services. However, such data may also serve to prevent commercial risks, for instance by denying access to customers who are suspected of jeopardising a company’s profits or reputation.

From a broader sociological viewpoint, we may see surveillance as a form of social control and necessary for communities to function. Even the smallest social groups set and monitor norms and will correct or exclude deviants who are unwilling or unable to adhere to them. Norms are not determined objectively but result from a definition process. Although philosophers such as John Stuart Mill and Joel Feinberg have tried to formulate universal liberty limiting principles, these in the end all depend on how social groups define concepts such as harm, paternalism or offense. Of course, some norms, such as not killing other members of the group, are universal. Most, however, are not and differ substantially between social groups. We have no way to objectively determine which norms are “better.” Therefore, we are left with two options: either allowing socially, economically and politically dominant powers to set the rules, or accept a certain level of deviance. Democratic societies will generally choose the latter option, not in the least because diverting from existing norms is often essential for scientific, economic and cultural progress, and for the general well-being of large societal groups: nobody can be non-deviant at all times.

When instruments of surveillance are applied in a targeted way, for instance to investigate crimes or to improve a product, in compliance with the Code of Criminal Procedure and data protection laws in general, there is no essential reason to be opposed against it. However, fundamental problems occur when instruments of mass surveillance are applied to search for deviance preventatively. No matter how sophisticated big data analysis will become, without an exact understanding of what constitutes deviant behaviour, such analysis will always be flawed and bound to produce large amounts of errors, particularly false positives, as well as undesired societal outcomes which may put several United Nations’ Sustainable Development Goals at risk.

Next, in Sect. 2, I will briefly outline the main drivers of mass-surveillance. Section 3 then addresses surveillance from a criminological viewpoint in more detail. Section 4 delves deeper into the question how social groups define deviance. Section 5 describes the problems of profiling and false positives. Section 6 concludes this chapter by looking at the impact of mass surveillance in the context of the UN’s sustainability goals.
2 The Growth of Surveillance

Scholars have identified different and sometimes mutually reinforcing explanations for the increase of the need of surveillance. First, it has been associated with economic structures and modernisations. Others have emphasised the impact of shocking events, particularly the attacks on the World Trade Centre and the Pentagon on 9 September 2001, and the calls for protection that followed from it. Third, developments in information and communication technology have made mass surveillance much easier and encompassing.

Michel Foucault pointed at the transitions caused by industrialisation and emphasised the need of disciplining the workforce for the emerging factory system (Foucault 1977). This required keeping the working classes under surveillance, which did not just involve enforcement and prisons, but an entire array of corrections of deviant behaviour, for instance in schools, the workplace itself, hospitals, and the military. However, in the early 1990s, the concept of discipline seemed to have lost relevance, as societies became ever more diversified and complex. The factory model no longer dominates modern societies and disciplining citizens into this mould is now less necessary. In addition, because of individualisation and migration, the number of subcultures has massively increased. Therefore, in his essay “Post-script on the Societies of Control” French philosopher Gilles Deleuze argued that the need for control has replaced the need for discipline (Deleuze 1992).

Ulrich Beck has argued that the process of technical modernisation itself caused dramatic changes to western culture and has resulted in a wide range of humanly produced risks (Beck 1992). This “risk society” too revolves around the need to control social, political, ecological and individual risks. More importantly, since in the early eighties the economic paradigm of neoliberalism became dominant in the Western world, policies based on it have vastly increased feelings of uncertainty regarding vital human needs such as a sustained source of income; affordable housing; that education will produce better chances in life; and a safe and unpolluted environment in general. Such uncertainties are reflected in a desire to minimise the risk of any sort of harm imaginable, either real or perceived (Ericson 2007). Although advocates of neoliberalism have continuously called for deregulation, in fact the opposite has occurred (Ayres and Braithwaite 1992; Power 2004). Indeed, the free market ideology calls for all sorts of control to keep markets fair and competitive, and to facilitate safety measures (Ericson 2007). Boutellier (2003) defined this inherent paradox as a ‘safety utopia’: individuals and corporations at the same time wish to enjoy maximum freedom and maximum governmental protection against any potential harm that may result from it.

Shocking events may accelerate this process. Societies have always responded to these with collective moral outrage and a passionate desire for vengeance (Garland 1991). For enforcement agencies, their ability to catch and punish the offenders was for a long time sufficient to restore faith in the protective function of the government. In modern society however, emphasis has increasingly shifted to prevention and protection. Particularly acts of terrorism result in calls for better surveillance of those
who might be a threat. Already in the 1970s, the German authorities replied to attacks by the *Rote Armee Fraktion* and other contemporary terrorists with *Rasterfahndung*, a concept to take data automatically from different databases to search for persons with specific risk profiles (Muller and Petit 2008). However, Al Qaida’s attacks on the United States in 2001, truly stimulated, and perhaps even more importantly, legitimated, the acceleration and expansion of surveillance trends (Ball and Webster 2003). From Edward Snowden’s revelations we first learned of the extent that domestic surveillance by the U.S. National Security Agency had grown into (Sherer et al. 2018).

In recent decades, rapid development of digital techniques has enabled to collect, store and analyse personal data on an unprecedented scale (Ball and Webster 2003). Furthermore, the Internet promoted globalised surveillance (Ball and Murakami Wood 2013). Digitalisation did not just widen the opportunities of States to collect data on their citizens. More importantly, it enabled private actors to gather massive amounts of personal and behavioural information on customers. Particularly “Big tech” corporations such as Google, Facebook and Amazon have become notorious in this respect, but nowadays almost every company that offers products and services which connect to the Internet will gather such data, and may apply it for other commercial purposes than “improving customer experience.” Corporations that once started with missions to connect people or to provide the best web search engine, quickly discovered that their most valuable asset was the information that they collected from those who used their services (Zuboff 2019). Big tech companies have increasingly expanded their operations by buying up other platforms and combining different streams of data. Their ambitions do not stop there, which is illustrated by Amazon’s plans to engage in for instance food distribution and healthcare, and Facebook led plans to launch the “Libra” as its own cryptocurrency (Rawnsley 2018; Paul 2019).

For a long time, corporations have done so in what is called ‘ungoverned space’ (Clunan and Trinkunas 2010). This refers to a context in which few regulations exist, and when they do, for example, in the shape of data protection laws, enforcement is highly problematic (Zuboff 2019). Shoshanna Zuboff introduced the term ‘surveillance capitalism’ to describe the effects of these developments, which she defined in a number of ways. At best it represents a new economic order that claims human experience as free raw material for hidden commercial practices of extraction, prediction, and sales. However, it can also be defined as a movement that aims to impose a new collective order based on total certainty. At its worst, surveillance capitalism will fundamentally change societies and the behaviour of people.

Surveillance researchers particularly worry about the blurring of the boundaries between public and private sector organisations (Haggerty and Ericson 2000; Ball et al. 2012). Indeed, personal and behavioural data collected by private companies, has become increasingly important for intelligence and enforcement agencies, not just for solving crimes, but also for profiling and prevention.
3 Surveillance from a Criminological Perspective

From a criminological perspective, we may look at surveillance in several ways. Mainstream criminologists may be interested in the motives and activities of persons and legal entities who are involved in illegal surveillance practices. “Critical” criminologists may also want to include behaviour that is as such lawful, but does cause blameworthy harm (‘lawful but awful’). Criminologists also look at the process of surveillance, which data is collected, where it ends up, whether surveillance is an effective tool to curb crime, and at enforcement of regulations. Finally, criminologists may want to explore structural drivers of illicit and harmful surveillance practices, such as protecting the interests of economically and politically powerful actors. Here, I will look at how surveillance data may be used for specific purposes. This section addresses five main categories, although these may overlap to some extent. The first is the use of surveillance data to commit crimes or cause harm; second is its use to solve crimes; third its use to prevent crimes, including acts of terrorism; fourth, to protect the interests of the powerful; fifth for private actors to gain corporate economic advantages.

To begin with, criminals and terrorists may acquire access to surveillance data and use it to facilitate illegal or otherwise harmful activities. Burglars might for instance gain access to data that ‘smart’ devices send to their manufacturer, and learn the times when nobody is present at specific addresses. Groups of car thieves would for instance be able to better target their operations if they can track vehicles of specific models and types. They may be able to hack into these data streams, but perhaps these are also for sale on the “Dark net” or from legitimate companies. Indeed, third parties may, in violation of contracts, use data for other purposes than for which it was originally made available, for instance not to provide specific commercial services, but for influencing the outcome of elections. In some cases, surveillance data which is potentially useful for criminals or terrorists, may be openly available. One example was fitness tracking app Strava, which collected GPS-data to allow runners to monitor their exercises, and unintentionally gave away the locations of secret U.S. military bases after tracking data had been published online (Hern 2018). The newest technological developments known as “deep fake” are particularly disturbing. These allow for instance to mimic someone else’s voice if one possesses just a few minutes of audio and to manipulate videos. Recently, criminals already used it to have a manager of a UK-based energy company transfer €220,000 to their account, because he thought it was the German chief executive of the parent company who gave him the order by telephone (Stupp 2019).

Surveillance data may, second, be used to solve crimes after these have been committed, or to gather evidence in situations in which illegal activities are ongoing. This for instance refers to the use of listening devices in cars and private homes, interception of telephone conversations or tapping of IP-addresses, physical surveillance of suspects, installing of cameras to monitor specific premises, and controlled deliveries of shipments of for example narcotic drugs. Modern criminal law enforcement agencies will possess the necessary training and certified equipment to use
these methods in confirmation with the Code of Criminal Procedure. However, law enforcement agencies also and increasingly rely on information gathered by private actors. An obvious example is the use of recordings of CCTV-cameras citizens and companies have installed to protect against burglary and theft. When some 25 years ago the use of mobile telephones started to become widespread, telephone operator’s traffic and location data quickly became an important source of information for investigative authorities (Spapens 2006). Since then, criminals have continuously sought for ‘safe’ means of communication, but usually without long-term success. For instance, Dutch criminals for a number of years sent text messages via Pretty Good Privacy (PGP) software installed on mobile phones. This worked until Dutch police seized and cracked the servers on which millions of messages were stored. Since then the information helped to solve a variety of cases, including underworld liquidations (Meeus 2017). More recently, normal people’s smartphones, combined with the data gathered by tech companies through installed apps and stored on their servers, have become an important tool to help solving crimes. In a recent murder case, a location app allowed the Dutch police to exactly reconstruct the victim’s as well as the suspect’s whereabouts and thereby solve the case. Finally, financial information kept by banks and other financial service providers has become hugely important for investigation agencies.

The third main purpose of surveillance is to prevent crime. To begin with, the fact that a person is aware of the chance of being watched, this may as such have a direct preventative effect because it increases the threshold for potential offenders. When CCTV-cameras in public areas were first introduced in the 1990s, it was expected that these would contribute to crime prevention. Analysis does indeed show a positive albeit modest effect, depending on the type of crime. CCTV-surveillance does reduce for instance vehicle crime, but has no effect on violence and assault (Bowers and Johnson 2016). More indirectly, surveillance data may be used to identify potential criminals and terrorists. Intelligence agencies, such as the General Communication Headquarters (GCHQ) in the United Kingdom and the National Security Agency have collected signals intelligence for decades, although their focus was not on preventing ordinary crime. After the fall of the Iron Curtain in 1989, western intelligence agencies were starting to partly shift attention to organised crime, mainly because of the perceived emergence of ‘organised crime multinationals’ such as the Italian Mafia and Russian ‘Mafiya’ (Andreas and Nadelmann 2006). However, organised crime researchers soon debunked the assumption that such syndicates were systematically setting up shop all over the world (van Dijk and Spapens 2013). In the mid-1990s, intelligence agencies changed focus to terrorism, and particularly after the attacks on the World Trade Centre in 2001 crime largely dropped from their agendas.

In the early 1990s, the police became aware of the potential added value of Intelligence Led Policing (ILP). Although the concept is not defined exactly, it generally reflects a shift from reactive to proactive ways of addressing crime problems. It involves collecting and analysing information about crime patterns to create intelligence products to assess potential problems (e.g. offenders, victims, contexts) and target resources to disrupt the most serious offenses and offenders
(Carter 2009; Ratcliffe 2008; Gibbs 2016). Although the concept is as such broader, it does encompass identifying unknown criminals and threats, based on personal and behavioural profiles. However, experiences in the Netherlands show that it is extremely difficult to draw up such profiles (see below).

Fourth, surveillance may be conducted to serve the interests of the powerful. Traditionally, rulers, particularly of non-democratic states, have had a keen interest in spotting all sorts of suspicious behaviour that might pose a threat to their reign. There are many historical examples, such as Napoleon’s France in the eighteenth century and Stalin’s Soviet Union in the 1930s.

Classical methods of information gathering such as the use of secret agents, informers and agents provocateurs, have over the years been supplemented with technical surveillance systems. Here too, recent developments in digitalisation have further expanded the toolbox of control. The use of facial recognition software and ‘smart’ cameras in public places, which may be further combined with all sorts of private sector data, illustrates this (Kobie 2019). Surveillance is increasingly globalised and thus also allows foreign states to scrutinise citizens in other countries. For example, the Eritrean government allegedly keeps a close watch on nationals who have fled the country, to prevent them from engaging in activities which might pose a threat to the regime (Opas and McMurray 2015). Criminologically, we may approach such use of surveillance data from the perspective of State crime (Chambliss 1989). This approach refers to acts by actors within the state that results in violations of domestic and international law, human rights, or systematic or institutionalised harm of its or another state’s population (Green 2004).

Fifth, surveillance serves corporate economic purposes. Here, I will focus on activities that cause blameworthy harm. To begin with, the data may result in social exclusion if it is used to detect potential risks, to the extent that it may become impossible for anyone with even the slightest perceived flaw to find a job, a house or a partner. Next, corporations may, like totalitarian states, engage in targeted surveillance of people they perceive as a threat. Recently it was revealed that agrochemical corporation Monsanto operated an intelligence center to monitor and discredit journalists and activists. Monsanto for instance targeted journalist Carey Gillam, who wrote a critical book on the company, and singer Neil Young, who released a critical album. The company allegedly paid Google to promote search results for ‘Monsanto Glyphosate Carey Gillam’ that criticised her work (Levin 2019). Finally, we may question whether data gathering for improving customer experience is necessary to the extent applied. Is it really essential that modern cars’ systems collect and send information on your driving style and locations history to the manufacturer, as well as to third parties (Markey 2015)? Do smart TVs constantly need to track what their owners are watching and relay it back to the TV maker and/or its business partners, to improve the product (Popken 2018)?

This section has illustrated the different criminologically relevant issues of surveillance. The techniques may be helpful to commit different types of cybercrime, either by mainstream criminals or corporate offenders, to which enforcement agencies must respond. Conversely, surveillance data may also help to solve crimes, and the examples shown above underline the increased importance of data.
collected by private actors for targeted investigative purposes. Of course, private as well as state actors must safeguard against the leaking of surveillance data to criminals and terrorists, and in criminal investigations surveillance data must be gathered and used in accordance with adequate requirements set in the Code of Criminal Procedure. However, from a criminological viewpoint, problems with surveillance become fundamental when it is applied for predictive policing, in other words to identify and prevent potential threats, and from a broader perspective, deviance. In the next sections, I will address these problems.

4 The Problem of Defining Deviance

If one wants to scrutinise people to detect deviant behaviour, the premise is that one knows how to define it. For harnessed mainstream criminologists this would not be a topic of much debate: deviance is simply behaviour in violation of what is adopted in the nation’s penal code. However, this narrow definition of the object of study of criminology poses problems when we look at modern day surveillance, because it goes far beyond of what is criminalised and also encompasses perceived violations of unwritten social norms. Deviance as such is roughly defined as behaviour that differs from a wide range of societal norms and rules. This raises the question how such norms are determined, and by whom.

The first approach, known as absolutist, assumes that the basic norms of a society are clear and obvious to all members of society in all situations. At the end of the nineteenth century, Emile Durkheim introduced the term collective conscience to refer to widely held social values and beliefs (Durkheim 1964). He reasoned that all behaviour which offends basic normative standards could be considered deviant, and thus be criminalised. Of course, general norms and values exist which are common to all societies, but these cover only a small part of what communities consider deviant behaviour. If we assume that a collective conscience exists, the norms which follow from it will reflect the moral values of the middle class and disregard the complexity of modern societies and the differences between a wide range of subcultures.

This is illustrated by early attempts to survey people’s opinions on what constitutes deviant behaviour. Theoretically, such an approach would render an objective picture, but in practice the results are very difficult to interpret. In a classic study, Simmons (1965) asked 180 people what they considered deviant behaviour. It resulted in 1100 different answers, falling into 250 categories. Of course, murder and theft were considered deviant behaviour, but also pacifists and working females. The problem is that almost all human behaviour will be considered deviant by someone and counting does not answer the question whether these opinions are morally defendable.

Howard Becker posed that acts become deviant if others respond to them as such (Becker 1963). However, there cannot be a proper response if deviant behaviour remains unknown. Furthermore, massive expression of public disapproval of deviant
behaviour is usually limited to shocking events, which are not necessarily the most harmful if we include long-term effects, for example, pollution. Another problem is that if communities do not respond to behaviour which is essentially deviant from a moral perspective, it will become normalised. In practice however, social groups will largely ignore what other subcultures consider deviant, as long as their behaviour does not harm or restrict them.

These examples underline that deviance has no ontological reality, but is instead socially constructed. The idea of social construction is rooted in symbolic interactionism, an approach which focuses on the way language and other types of interaction structures how people experience, interpret and attribute meaning to everyday reality (Blumer 1969). Communities thus also construct social norms. A social norm is ‘any standard rule that states what human beings should or should not think, say or do under given circumstances’ (Blake and Davis 1964). These norms are continuously defined and redefined by the members of a given group.

In larger communities it is impossible to constantly discuss and define norms in personal interactions, simply because not every member of a large social group can maintain contact with all the others. Instead, norms are “informally codified” in culture. Culture can be seen as norms that are commonly accepted without need of debate. Religion may also be viewed as a way of codifying cultural norms, in this case in the shape of religious texts and their interpretation, and rituals in which religious norms are learned and explained. Finally, laws can be viewed as formal codifications of societal norms.

Norms are necessarily simplified representations of the complexities of everyday life. In specific situations, there may be many reasons why general norms would perhaps not apply. These are, in other words, the product of a process of simplification known as framing. Frames themselves are the result of a definition process, in which individuals, interest groups, institutions, political parties, religious actors, the media—increasingly also social media—as well as science, interact. The process takes place at different levels: local, national and international. Because the process is continuous, notions about deviance are not static, but change over time. Furthermore, they differ across and within societies. A fundamental problem is that the ability to engage in definition setting is spread unevenly. Economically powerful actors are inherently better placed to influence the process, for instance through the lobbying of politicians, funding of research, and feeding the media.

Paradoxically, the Internet did make it easier for individuals to exert definition power. Think for instance about influencers with large followings on Facebook or YouTube. Another example is Greta Thunberg, a now 16-year old who was catapulted from being a schoolgirl who sat down in August 2018 in front of the Swedish parliament with a cardboard sign telling she was on strike because of the climate, to addressing the United Nations about the subject little more than a year later. The Internet, however, also further complicated the process of definition setting because the number of specialised communication channels has exploded, and ‘bubbles’ occur that distort the interactive process. Furthermore, the boundaries between the local and global have faded, and actors from all over the world may now try to influence local definition setting.
As I have noted above, surveillance is an instrument of social control: communities use it to detect deviant behaviour and thus to uphold social norms. However, if we cannot objectively determine what deviant behaviour is, we are also unable to define what should become the target of surveillance.

5 The Problem of False Positives

A fundamental question of assessing deviance and thereby the objectives of surveillance is how to avoid false positives. In this context false positives can be defined as behaviour which is not malicious, whereas this cannot be established correctly based on comparative data analysis.

Of course, for totalitarian regimes false positives are not much of a concern: even the slightest sign of discontent may be enough reason to be marked as a threat and carted off to prison or to an ‘education and training centre’ (Allen-Ebrahimian 2009). For example, how many of the millions who were sent to the Gulag or killed by the Stalinist regime in the 1930s, represented a real danger to communism?

For economic actors the problem of false positives is more ambiguous. On the one hand, better predictions allow for better sales. On the other, advertising companies may be less concerned if they spam someone who is not interested. People may indeed be annoyed about being false positives when they receive adds for paracetamol after tapping in ‘headache’ in a search engine, or maybe worse, an offer to get insurance for your funeral, but will usually not complain. However, false positives do become problematic when the result is denial of access to specific services.

By comparison, for democratic state actors, avoiding false positives is a key issue when it comes to preventing crime. Criminologists have addressed the errors problem extensively in the context of predicting recidivism. Although prediction methods were able to identify certain groups of offenders having a higher-than-average statistical probability of recidivism, these methods showed a disturbing incidence of false positives: for violent crimes, at least two false positives for every true positive (Monahan 1981). Such mistaken forecasts could be gravely damaging to the individuals involved, for they could lead to their prolonged incarceration (Von Hirsch 1998).

More recently, researchers have for instance looked at surveillance measures intended to prevent terrorist attacks. One example is the No Fly Lists, with thousands of names of people who should be denied to board flights into and out of the USA. A large number of false positives have mistakenly been denied access and missed their flights (Bjørgo 2016). Another example is programs to encourage the public to report suspicious behaviour. It will not come as a surprise that citizens consider a wide range of behaviour ‘suspicious’, especially when it concerns minorities. In 2006, for example, six Muslim imams were removed from a US Airways flight because passengers thought they were a threat to their safety (Larsen and Piché 2009). The problem is not just confined to serious threats such as terrorism, as anyone who takes
part in a neighbourhood WhatsApp group to report suspicious behaviour, will be able to confirm.

From a technical point of view, one might argue that the problem of false positives can be solved by developing better profiles to base surveillance on. Indeed, personal and behavioural data is often lacking in government databases. In 2012, I was involved in a project in which a profile was composed based on the characteristics of the most notorious criminals in the city of Amsterdam. It took a massive effort to integrate the different databases from which we took this information and be able to run the profiles. Government databases had mainly been developed further from mid-1990s software, and had not been set up with the aim of interchangeability. When we finally were able to run the parameters through the integrated database, a substantial number of persons matched the profile, but were hitherto unknown to the authorities. Were they indeed very smart criminals who had so far managed to completely stay under the radar? Of course not: all ‘hits’ turned out to be false positives.

Critics may argue that the attempt was primitive, considered the amount of information which private entities currently have available, such as search histories, financial transactions, movements, social networks, and postings on social media platforms. Using this information would indeed allow construction of highly detailed profiles, but we still would not know which variables would be relevant from the perspective of detecting deviance. The range of potentially deviant behaviour is simply far too wide to apply general profiles. However, narrowing down the profiles to very specific behaviour will inevitably be perceived as discriminatory and stigmatising to specific population groups (Bjørgo 2016).

More importantly, because the persons who build the profiles of deviance cannot refer to an objective list of what to include as ‘suspicious’ they have only three options, or combinations of these. The first is simply to follow Durkheim in his assumption that a collective conscience exists and draw up a list of deviant behaviour based on one’s perception of it. The problem is that this will result in profiles which are highly biased to the perceptions of the persons who construct them. The second is to use ‘self-learning’ software which searches for inappropriate content which is similar to what was previously considered deviant, or characteristics of criminals. However, this too requires labelling specific behaviour as deviant before you can find something similar, or to be able to determine what constitutes a criminal, and therefore does not solve our problem. The third option is to search for anomalies. Unfortunately, this also requires that we must know which anomalies are to be considered risky or suspicious.

For all sorts of reasons, public and private surveillance operators have successfully created the impression that their profiling systems are infallible, objective, reliable and accurate in the assessments that they produce (Yeung 2018). They are not. Indeed, Netflix may have little difficulty in offering you content similar to what you watched before. This does not require much sophistication, and as argued above, getting it wrong does not cause much harm. And of course, it does not point you to what you are really interested in: something challenging and new that you did not think of before. Accurately predicting the threat someone represents to societal
order, based on personal and behavioural characteristics is another matter. If we
allow powerful economic or state actors to define what is deviance, this will
inevitably result in biased and inaccurate profiles that generate large amounts of
errors (Korff and Browne 2013). The impact on society cannot be underestimated. In
the next section, I will sum up the issues in the context of the United Nations’
sustainability goals.

6 Conclusion: The Impact of Mass Surveillance
and the UN’s Sustainability Goals

Researchers in the field of surveillance studies have often referred to the negative
impact of mass surveillance from the perspective of its panopticon effect (Haggerty
and Ericson 2000). The idea of the panopticon was originally defined by nineteenth
century philosopher Jeremy Bentham as a prison design which would theoretically
allow a single guard to keep all prisoners under surveillance, who at the same time
were unable to either see each other, or know when they were watched. The intended
effect was to discipline: the fact that one could be watched at any given time but not
necessarily all the time, would be enough to encourage inmates to behave correctly.
Although the panopticon prison was never built, the idea did exert substantial
influence on prison design. In the 1970s, Michel Foucault transposed the panopticon
idea to society as a whole (see above, Foucault 1977). Whether or not one wants to
use the panopticon metaphor, the impact of living in a society where everybody is
kept under constant surveillance is substantial, particularly when it is hard to tell
what will be considered deviant behaviour now or in the future, and by whom.

The risk is a “chilling effect” in which citizens will be afraid to speak out or
display any behaviour which might be considered inappropriate (Haggerty and
Ericson 2000). This may result in mistrust, and people hiding their true selves.
Some of my students for instance explained that they maintain two accounts at
Instagram: one in which they pose as virtue itself that they may present when a
prospective employer or landlord demands access, and another where they post their
real life.

Not risking to be deviant will eventually also affect economical, scientific and
cultural progress. Throughout history, many crucial innovations have been consid-
ered deviant at first, such as Copernicus’s idea that the earth and the other planets
revolve around the sun, instead of earth being the centre of our solar system. Large
numbers of writers, painters and other artists we hold in high esteem today, have in
their time been confronted with disapproval of their work, and may have even been
prosecuted for it. The fact that democratic societies are able to allow a certain level of
deviance, helps to explain their success, and why they attract so many people from
nations which do not allow the same levels of freedom. In conclusion, the ‘chilling
effect’ of mass surveillance may put at risk sustainable development goals related to
ensuring good health and—mental—well-being (SDG 3) decent work and economic growth (SDG 8); and industry, innovation and infrastructure (SDG 9).

The second problem I identified also follows from the fact that we cannot objectively define deviance, and causes that any attempt at profiling and finding threats through mass surveillance will result in large numbers of false positives. In practice, this problem is aggravated by the fact that powerful private actors increasingly determine what is to be considered deviant. This will inevitably result in bias and social inequalities. An employer may for instance impose surveillance on workers to find out whether they use drugs or regularly drink alcohol, to prevent safety hazards, but the company management will itself be undoubtedly exempt from such requirements although their decisions are potentially far more harmful to people’s lives. As we have seen above, it is usually minorities and other less-powerful groups in society who are considered to be a threat when it comes to for instance crime and terrorism. However, criminologists have underlined time and again that corporate deviance causes much more injury, death and financial harm, although it is often not seen as shocking criminal behaviour. Mass surveillance impacts unevenly on societal groups, and threatens the development goals of reducing inequalities (SDG 10) and promoting peace, justice and strong institutions (SDG 16).

Although the public has become increasingly aware of the fact that mass surveillance exists, and because of hit series such as “Black Mirror,” so far not much seems to be changing in their daily practices. Perhaps the main reason is submission to the notion that being under constant surveillance cannot be avoided (Romele et al. 2017). But maybe we do see some gradual changes. The big Tech companies are increasingly the object of governmental scrutiny, for instance because of misuse of their monopoly positions, problems with data protection, and tax avoidance. In 2017, the European Commission imposed a fine of €2.4 Billion on Google for unfairly favouring some of its own services over those of rivals (Scott 2017). In September 2019, 50 U.S. states and territories announced to investigate Google’s alleged monopolistic practices (Romm 2019). So far, big Tech has been quite successful at fencing off effective regulation of its harvesting of user data (Zuboff 2019). Whether this situation will continue remains to be seen. For the good of the global community, an approach similar to how the early twentieth century ‘robber barons’ were contained, through breaking up monopolies on the one hand and effective regulation on the other, should perhaps now be applied to the modern ‘robbers of personal data’, if we aspire to fulfil the UN’s Sustainable Development Goals.

References

Allen-Ebrahimian, B. (2009, November 24). Exposed: China’s operating manuals for mass internment and arrest by algorithm. *International Consortium of Investigative Journalists.*

Andreas, P., & Nadelmann, E. (2006). *Policing the globe: Criminalization and crime control in international relations.* New York: Oxford University Press.
Ayres, I., & Braithwaite, J. (1992). *Responsive regulation: Transcending the deregulation debate*. New York: Oxford University Press.

Ball, K., Haggerty, K., & Lyon, D. (Eds.). (2012). *Routledge handbook of surveillance studies*. London and New York: Routledge.

Ball, K., & Murakami Wood, D. (2013). Editorial. The political economy of surveillance. *Surveillance & Society, 11*(1/2), 1–3.

Ball, K., & Webster, F. (2003). The intensification of surveillance. In K. Ball & F. Webster (Eds.), *The intensification of surveillance. Crime, terrorism and surveillance in the information age* (pp. 1–15). London: Pluto Press.

Beck, U. (1992). *Risk society: Towards a new modernity*. London: Sage.

Becker, H. (1963). *Outsiders: Studies in the sociology of deviance*. New York: The Free Press.

Bjørgo, T. (2016). *Preventing crime. A holistic approach*. Basingstoke: Palgrave Macmillan.

Blake, J., & Davis, K. (1964). Norms, values, and sanctions. In R. Faris (Ed.), *Handbook of modern sociology* (pp. 456–484). Chicago, IL: Rand McNally & Company.

Blumer, H. (1969). *Symbolic interactionism: Perspective and method*. Englewood Cliffs: Prentice-Hall.

Boutellier, H. (2003). *De veiligheidsutopie*. The Hague: Boom Juridische uitgevers.

Bowers, K., & Johnson, S. (2016). Situational prevention. In D. Weisburd, D. Farrington, & C. Gill (Eds.), *What works in crime prevention and rehabilitation* (pp. 111–135). New York: Springer.

Carter, D. (2009). Law enforcement intelligence: A guide for state, local, and tribal law enforcement agencies (2nd ed.). Office of Community Oriented Policing Services, U.S. Department of Justice: [http://fas.org/irp/agency/doi/lei.pdf](http://fas.org/irp/agency/doi/lei.pdf)

Chambliss, W. (1989). State-organized crime. *Criminology, 27*(2), 183–208.

Clunan, A., & Trinkunas, H. (2010). *Ungoverned spaces*. Stanford, CA: Stanford University Press.

Deleuze, G. (1992). Postscript on the societies of control. *October, 59*(Winter), 3–7.

Durkheim, E. (1964). *The division of labor in society*. New York: Free Press.

Ericson, R. (2007). *Crime in an insecure world*. Cambridge: Polity Press.

Foucault, M. (1977). *Discipline and punish: The birth of the prison*. New York: Vintage.

Garland, J. (1991). Sociological perspectives on punishment. *Crime and Justice, 14*, 115–165.

Gibbs, C. (2016). Addressing transnational environmental crime: The role of intelligence led policing. In T. Spapens, R. White, & W. Huismann (Eds.), *Environmental crime in transnational context* (pp. 85–100). London and New York: Routledge.

Green, P. (2004). *State crime: Governments, violence and corruption*. London: Pluto Press.

Haggerty, K., & Ericson, R. (2000). The surveillant assemblage. *British Journal of Sociology, 51*(4), 605–622.

Hern, A. (2018, January 28). Fitness tracking app Strava gives away location of secret US army bases. *The Guardian*.

Kobie, N. (2019, June 7). The complicated truth about China’s social credit system. *Wired*.

Korff, D., & Browne, I. (2013). *The use of the Internet & related services, private life & data protection: Trends, technologies, threats and implications*. Council of Europe, T-PD (2013)07.

Larsen, M., & Piché, J. (2009). Public vigilance campaigns and participatory surveillance after 11 September 2001. In S. Hier & J. Greenberg (Eds.), *Surveillance: Power, problems, and politics* (pp. 187–202). Vancouver: UBC Press.

Levin, S. (2019, August 8). Revealed: How Monsanto’s ‘intelligence center’ targeted journalists and activists. *The Guardian*.

Markey, E. (2015). *Tracking & hacking: Security & privacy gaps put American drivers at risk*. Published online at: [markey.senate.gov](http://markey.senate.gov)

Meeus, J. (2017, June 6). Hoe justitie 3,6 miljoen versleutelde berichten van criminel ontcijfert, [nrc.nl](http://nrc.nl).

Monahan, J. (1981). *Predicting violent behavior: An assessment of clinical techniques*. Thousand Oaks, CA: Sage.
Muller, E., & Petit, G. (2008). Strategieën tegen Terrorisme. In E. Muller, U. Rosenthal, & R. de Wijk (Eds.), Terrorisme: Studies over Terrorisme en terrorismebestrijding (pp. 271–308). Deventer: Kluwer.

Opas, M., & McMurray, D. (2015). Under the gaze of the state: ICT use and state surveillance of Eritrean refugees in Italy. Refugee Survey Quarterly, 34(4), 105–125.

Paul, K. (2019, June 18). Libra: Facebook launches cryptocurrency in bid to shake up global finance. The Guardian.

Popken, B. (2018, February 7). Your smart TV is watching you watching TV, Consumer Reports finds. Nbcnews.com

Power, M. (2004). The risk management of everything: Rethinking the politics of uncertainty. London: Demos.

Ratcliffe, J. (2008). Intelligence-led policing. Portland, OR: Willan.

Rawnsley, A. (2018, March 25). Politicians can’t control the digital giants with rules drawn up in the analogue era. The Guardian.

Romele, A., Gallino, F., Emmenegger, C., & Gorgone, D. (2017). Panopticism is not enough: Social media as technologies of voluntary servitude. Surveillance & Society, 15(2), 204–221.

Romm, T. (2019, September 10). Google target of antitrust investigation led by 50 U.S. states and territories. Nationalpost.com

Scott, M. (2017, June 27). Google Fined Record $2.7 Billion in E.U. Antitrust Ruling. The New York Times.

Sherer, J., Sterling, N., Burger, L., Banaschik, M., & Taal, A. (2018). An Investigator’s Christmas Carol: Past, present, and future law enforcement agency data mining practices. In H. Jahankhani (Ed.), Cyber criminology, advanced sciences and technologies for security applications (pp. 251–273). Switzerland: Springer.

Simmons, J. (1965). Public stereotypes of deviants. Social Problems, 13(2), 223–232.

Spapens, T. (2006). Interactie tussen criminaliteit en opsporing. Antwerp and Oxford: Intersentia.

Stupp, C. (2019, August 30). Fraudsters used AI to mimic CEO’s voice in unusual cybercrime case. The Wall Street Journal.

van Dijk, J., & Spapens, T. (2013). Transnational organized crime networks across the world. In J. Albanese & P. Reichel (Eds.), Transnational organized crime. An overview from six continents (pp. 7–27). Thousand Oaks, CA: Sage.

von Hirsch, A. (1998). Penal theories. In M. Tonry (Ed.), The handbook of crime and punishment (pp. 659–682). Oxford University Press.

Yeung, K. (2018). A study of the implications of advanced digital technologies (including AI systems) for the concept of responsibility within a human rights framework. Council of Europe. MSI-AUT(2018)05.

Zuboff, S. (2019). The age of surveillance capitalism. New York: PublicAffairs.

Toine Spapens is a Full Professor of Criminology at Tilburg University, the Netherlands. He received his PhD in criminology in 2006. Since the early 1990s, Spapens has made extensive empirical research on (organized) crime and its containment, international law enforcement cooperation, and environmental crime. His empirical work includes trafficking in illicit firearms, synthetic drug production, large-scale cannabis cultivation, illegal gambling and match-fixing, and waste and wildlife trafficking. His PhD focused on the question how criminals adapt to special investigative techniques used by enforcement agencies, such as surveillance and interception of communication. His recent projects concerned the use of administrative law, and powers to maintain public order, for the prevention and disruption of crime (2015); prevention of intergenerational transmission of delinquent behavior in families involved in organized crime (2017, 2020); and criminals who engage in philanthropic activities, through sponsoring of sports clubs and good causes (2018, 2019). In the context of environmental crimes and harms, Spapens co-edited the books Environmental Crime and Its Victims (2014); Environmental Crimes in Transnational Context (2016) and Green Crimes and Dirty Money (2018). E-mail: A.C. Spapens@tilburguniversity.edu.