Mareile Kaufmann and Heidi Mork Lomell

An introduction to digital criminology

"The Internet will disappear," is a famous sentence uttered by Eric Schmidt, then-Google CEO visiting the 2015 World Economic Forum (Smith 2015, online). His vision refers to the ways in which one day the devices surrounding us will be seamlessly connected, rendering our online existence from a deliberate choice into a default state. Indeed, being online is an everyday experience for many, where it tends to slip into the "technological unconscious" (Thrift, 2004). The same applies to our use of offline digital devices: it is easy to forget about their presence and to reflect about the ways in which they influence our everyday lives. Yet, even if unconscious, the internet and other digital infrastructures do not *disappear.* Not only can they be unintuitive, break down, or act back in unforeseen ways, disrupting our supposedly seamless experience. But their material existence keeps confronting us with societal and political issues. They raise questions about ownership (who owns infrastructures and data?), design (which values and functionalities are embedded in the design of digital devices?), practice (how do technologies enable new forms of usage?), choice (which choices can we take ourselves, which are taken for us?), ethics, governance, and regulation (what power structures and dilemmas does digitalization entail?).

This book pays attention to the ways in which electronic digital devices, online and offline, spread and cut across all fields of criminology. Criminologists need to be able to identify, make visible and analyze the technologies, practices, and social dynamics that emerge from their growing relevance. Digitalization changes interaction and information flow, speed and spatiality, experiences and practices of crime and crime control. It influences every aspect of criminology, such as victimization and violence, corporate and organized crime, fraud, drug markets and consumption, radicalization and terrorism, policing and forensics, sentencing and punishment. Digitalization bears new modi operandi, cultures of surveillance and social control, and new types of offenses, which this book documents and problematizes.

Hence, this is a handbook about the *digitalization* of criminological arenas rather than criminology in the 'digital era.' Criminology has not entered the 'digital age,' an epoch in which the digital—singular—is an entirely new and all-encompassing phenomenon. Rather, its theory, method, and subjects are part of a process of digitalization that is rooted in the discipline's original matters and spreads in manifold ways.

In what follows we will first go back to the origins of the word *digital* and show how it has shaped criminological work from its very beginning. We will then move on to describe the ways in which 'the digital' and its technologies have changed. Criminologists have to take account of these changes when they study specific phenomena, especially because the logics of digitalization tend to tie in with politics and power. Studying digitalization across different criminological fields also warrants a re-thinking of the tools we use for knowledge-making, which we will discuss before we let readers off to browse, delve into specific topics and plan research projects.

 https://doi.org/10.1515/9783111062037-001

Continuities

Maps, tables, sketches, specimen. Criminology has always had an intimate relationship to data and measurement. Like in any other empirical science, infrastructure such as spreadsheets, file cabinets, thermometers, and dictaphones are key to the generation, collection, and organization of criminological data. They are important artifacts in the making of criminological knowledge. Metric tools generate data, but they also act as data when one takes account of the ways in which measurement and counting vary across tools.

Crimes have been counted ever since society "became statistical" between 1820 and 1840, when an "avalanche of printed numbers" swept over many European countries (Hacking, 1990: 1–2), which also manifested itself in emerging governmental rationalities. So when numbers, enumeration, and statistics became part of social science—and governance—'crime' was understood, rendered, and approached in a new fashion (Lomell, 2010). From the beginning, numeric representations of social phenomena were used by social scientists to substantiate theories and to identify statistical laws and regularities, both in order to improve and control 'deviant subpopulations' (Lomell, 2011). Reading regularity and predictability into the first crime rates, Adolphe Quetelet [1796–1874] concluded that the causes of crime must lie outside of each individual's control, and that crime could not be a simple matter of individual choice (Quetelet, [1842] 1996). Crime as a *social* phenomenon—and problem—was invented with the representation of crime in numbers and the creation of the crime rate.

The criminological discourses of the early 1900s were also characterized by debates about the 'correct' instruments and methods for metricizing criminals (Gibson and Rafter, 2006). Today, in the 21st century, debates about measurement tools are not concluded. They may no longer refer to the process of rendering the bodies of criminals into numbers, but to the 'correct' choice of instrument for identifying patterns of crimes and risks. Relatedly, the ways in which criminological knowledge production impacts societies is also not a new discourse. For example, critics have long addressed the discriminatory nature of early metric works such as Lombroso's *Criminal Man* (Basaglia, 1971, cited in Montaldo, 2018). Yet, discussions about discrimination are still central in today's biometric projects (see Biometric Failure by Din and Magnet).

Though it is seductive to think of digital criminology as a new field, the above goes to show that criminologists have a long tradition of engaging (with) digital logics. For many, it may be unusual to think of the above practices of measurement and numbering as digital. The word *digital*, however, goes back to *digitalis*, measuring a finger's breadth, which came to denote discrete entities that can be used to count and calculate with. The discrete units of the abacus are, then, a form of digital information in an *analog* fashion. Yet, today's vernacular refers to digital information as the electronic representation of data in the discrete values of ones and zeros as established in the mid 20th century (see Digital by Wernimont). This conceptual development expresses the continuities that characterize digitalization: that digital technologies and practices

did not arise with the advent of the personal computer or the Internet. They are the result of more comprehensive genealogies.

The way in which *digitalis* relates to concrete, physical units reflects yet another important aspect: the materialities of digital data or digital matters. In the same way in which skulls, maps, and archives are material, electronic data and infrastructures, too, are material. That is to say: a software indicating crime hot spots is not only an extension of analog data, such as maps with needles and pins as prototyped by the Chicago School (Thrasher, [1936] 2013). Its electronic instance, too, is enabled and upheld by a network of humans, items, and material practices without which it cannot exist.

Digital criminology, then, does not refer to virtual and abstract phenomena (Floridi, 2010) or totalizing qualifiers such as 'ages' and 'worlds.' It engages with concrete matters that have specific genealogies. And these material genealogies keep evolving. Infrastructure studies provide a lens to understand these phenomena as evolving sociotechnical assemblages (see Infrastructures by Grisot and Parmiggiani). For instance, rather than studying electronic monitoring in prisons as a discrete technology, one can map the larger and evolving surveillance assemblages and infrastructures that it is part of.

Returning to the word *digitalis*—measuring a finger's breadth—we find yet more aspects that are relevant to defining digital criminology. The activities of measuring and calculation comprehended in *digitalis* have been a part of criminology long before electronic computation arrived. Adolphe Quetelet's correlational approach to crime mentioned above, the anthropometric system of Bertillonage, or Cesare Lombroso's typology of 'born criminals' are examples of measurement, numeric archives, and statistics that were a part of establishing criminology. They are examples of digital methods, of counting, measuring, and calculating with discrete units in the empirical research on crime. Even though biometrics is a word that we mainly associate with today's technologies for facial recognition and border control, Bertillonage is in fact one of the first biometric systems used in law enforcement. Data collection, profiling, pattern recognition as well as the drive for systematization and efficiency are logics that characterized early criminology and still form the basis of electronic digital practices today.

For example, the search for patterns of delinquency in urban environments (Shaw and McKay, 1972), the detection of regularities as performed in routines (Cohen and Felson, 1979) and rational choices (Cornish and Clarke, 1986) are metric and statistical approaches to crime that constitute the logics of predictive policing software today. Some software solutions actually incorporate such theoretical models into their algorithms where they are used to define parameters for the identification of patterns (note that an algorithm is a set of instructions to solve a problem via computation—electronic or not, see Algorithm by Leese). While patrol, too, has always been central to the police, as for instance with Sir Robert Peel's 'Bobby,' the use of advanced statistics led to a prioritization of specific environments over time. The growing amount of digital information available to private and public services as well as electronic computation now enable software-supported predictions (see Prediction by Ķīlis, Gundhus, and Galis). Such predictions are increasingly used to fine-tune police presence and the

prevention of expected crimes, which is captured in the term 'precision policing' (Shults, 2022).

The story of crime patterns, police patrol, and predictions, then, illustrates the ways in which a *digital* criminology involves genealogies, materiality, and calculus. What is more, the turn towards a 'politics of *pre-*' (Kaufmann, 2023), that is the management of security with a focus on the future (Zedner, 2007), was a process that did not arrive with big data and electronic computing, but was also rooted in the history of criminological practices. Think of the role of risk logics in criminal justice that existed long before sentencing was automated, involving large databases (Maurutto and Hannah-Moffat, 2006). Yet, arguably, the role of prediction and prevention became more manifest and integrated into crime control with the advent of the personal computer and digital archives. It is no longer only an *aspiration* to predict and get a sense of control over the future. The availability of predictive instruments suggests a new *responsibility* to predict, prevent, profile, target, and to be efficient. This new responsibility is firmly established in modern societies that are imbued with a preventive gaze, where "incidents are not perceived as tragic accidents, but instead as avoidable events" (Peeters, 2013: 22). The future will stay with us in the future. Prediction will remain a key logic in criminology, because it is "malleable enough to be adopted and adapted by several criminal justice actors, yet robust enough to maintain a common identity and concept across different organisational sites and applications," as Ķīlis and colleagues elegantly put it in their contribution (see Prediction by Ķīlis, Gundhus, and Galis, cf. Star and Griesemer, 1989).

Creating profiles of criminals, terrorists, or 'dangerousness' is another phenomenon that tends to be presented as an innovative, 21st-century security practice. But here, too, historical developments and continuities characterize today's trends. The practice of measuring and categorizing criminals, victims, and human behavior started in the early 1900s. Early biometric instruments set the trend to measure anything from head shape, weight, body build and to correlate it with behavior in order to arrive at a profile of criminals by type of crime. While modern profiling rarely seeks to predict behavior, the idea of using categories and profiles in order to control crime is as present as ever. Profiles are used, for example, to flag suspicious financial transactions, conspicuous browsing behavior, or to predict the skin color of a suspect from DNA (see DNA/Big Genome Data by Kaufmann).

For criminologists it is thus important to remember that digital technologies have a history and that criminological researchers are, to a certain extent, well-equipped to study digital technologies and practices. But it would be incorrect to claim that digitalization is a development without interruptions, jumps, and changes. As Roger Burrows puts it: "the 'stuff' that makes up the social and urban fabric has changed" (2009: 451).

Changes

If the 'stuff' that makes up digitalization has changed, the advent of electric power arguably introduced one of the most significant shifts. With a simple abacus, for example, one would be able to calculate multiplications of 10-digit numbers in one second. The British *Colossus*, the first programmable, electronic, digital computer, was used in World War II for cryptanalysis. By computing 5,000 operations per second, it was able to decrypt the German Lorenz cipher and changed the course of war. Since 2022 machines exist that are capable of calculating 10 to the power of 18 operations per second. Such supercomputers are in need of energy comparable to that of 16,000 homes (Johnson-Groh, 2023). Today's supercomputers, for example, simulate anything from the universe to nuclear weapons capabilities which form the basis for security politics of global dimensions and beyond. We can observe that electric power, powerful computing, and powerful political dynamics change together, something that is crucial to criminological analysis. But how do these shifts connect?

First, we can mention the phenomenon of *datafication* (see Datafication by Chan). The above examples show that ever-more aspects of life become captured as information, or to put it differently: informationalized or datafied. With the spread of digital infrastructures more objects, bodies and behavior become subject to measurement. More measurement activity generates more data, and vice versa. Datasets can be distinctive, specific, and small. But they can also be various, velocious, and voluminous. While we have not left filing cabinets and paper folders behind, electronic datasets have become so massive that their storage is a considerable percentage of global carbon emissions. Though their size is no longer graspable, which is why we like to call it 'the cloud,' we can still observe that data are material and create very concrete effects. 'Big data'-centers are so physical that they change the atmosphere and the 'stuff' needed for electronic technologies has led to a competition over metals, mining, and markets.

Unlike 'the cloud' suggests, electronic data are not ever-present, they are not everywhere. Some societies are heavily digitalized, while others are not. To some populations digital technologies are the foundation of their social lives, while others are excluded, underequipped, or disinterested. Nonetheless, digital data and technologies have grown in relevance to the extent that most people experience the effects of datafication. This has brought about technological innovation, but has also led to new crimes and harms, exponential surveillance and sousveillance.

A familiar example would be social media, which have become integral to many peoples' lives. Social media have reshaped social relations and politics, and thereby also crime and control (see Social Media by Twigt). They allow users to engage in harmful or illegal acts, such as online mobbing, grooming, or drug trade. Social media provide platforms for new social practices (e.g., sex work) and groups (e.g., incels). But they also generate new dynamics, such as political action, radicalization, control practices, and the resistance to control. Another example is the 'Internet of Things' (IoT),

which refers to the ability of everyday objects to connect to the internet, other communication networks, and each other to create a 'smart' environment (that is Google's vision mentioned above). These objects generate and exchange data via sensors and act based on data analysis. Many IoT devices, however, have not been designed with privacy and social implications in mind; they follow a technical, not a socio-technical approach to technology development. Needless to say that the IoT is per se a surveillance tool, which can be abused for both control and criminal purposes (see Internet of Things by Milivojevic). The IoT is also the base model for 'smart cities'—technologically sophisticated urban areas that use digital devices, data analytics, and innovative architectural design to overcome traditional metropolitan challenges such as traffic congestion, crime, and incivility. The ways in which such projects root entirely new surveillance infrastructures in societies, facilitating new forms of crime management, but also social control and types of crime, is a phenomenon of rising importance to digital criminologists (see Smart City by Hayward). In tandem with a rise of smart infrastructures we see a normalization and dispersion of digital borders that co-shape the politics of inclusion and exclusion, wanted and unwanted mobilities, and knowledge-making about moving subjects and dynamic territories (see Borders and Border Control by Jeandesboz).

Indeed, studying digitalization also means researching how data and technologies impact the *temporal and spatial dimensions* of criminological phenomena. Speed and heightened connectivity do not always imply sophistication or betterment. Rather, they redefine criminological fields of study in various ways. For example, marketplaces for drug trade still involve farms, cityscapes, and transport networks, but also online platforms, e-payment systems, and the 'darknet.' The darknet is a term adopted by law enforcement to describe those parts of the internet that are encrypted and layered to enhance privacy. With increasing digitalization drug markets may not necessarily become more global (in fact, many of them were dependent on global connections long before the rise of online drug markets), but digitalization leads to new forms of both closeness and distance. Sellers and buyers get in touch without having to leave their homes and the darknet changes the security of buyer–seller contact for better and worse. In addition, strategies for advertisement, negotiation, and feedback are adapted to digital markets. This example illustrates the complexities that electronic data and technologies bring to criminological phenomena.

To grasp the relationship between digitalization, crime, and crime control, then, it is important to understand the properties of digital devices and what they afford (Gibson, 1979). An affordance is that which enables and disables, encourages or discourages specific actions. Environments, objects, or artefacts do not cause behavior per se; rather, they offer, enable, or *afford* some actions over others. What technologies afford is a key entry point in understanding what humans can, and will, do with them (see Affordances by Wood and Arpke-Wales). Affordances are specific to each object. In digital criminology, entire research projects can be dedicated to studying the affordances of digital devices, how they change environments, practices, and other things. Such de-

vices can include computers and software, or credit cards and banking infrastructure, just to name a few.

In order to study the effects of digitalization more generally, it is helpful to understand the affordances of electronic digital data (Kaufmann and Jeandesboz, 2017). Above, we have pointed out that digital data are *discrete* (as opposed to continuous), which makes it easy to count, calculate, and measure with digital data. Hence, the digital character of electronic information is the basis for numeric and computing operations that are needed to run anything from local offline data programs to complex telecommunication platforms (see Computation by Mazzilli Daechsel). What is more, digital information can be *stored*, which means that we have archives of entirely new dimensions. Paper archives were the big data of the early 20th century. Today's big data and digital archives, too, are physical as they come in the form of hard disks and data centers. Actually, some of today's big datasets also involve paper forms that are translated into electronic data and across professional domains (see Translation by Wilson-Kovacs). The digitalization of archives, however, alters the answers to questions such as: Under which conditions are digital archives gathered and made available? Who governs them? And how do they reshape ontologies and epistemologies of crime and crime control? (see Archives by Thylstrup and Veel).

Digital archives make information *available* and *searchable* to different parties, which also means that it can be used for simple and complex analyses. Due to its electronic form, data are also *transferable* if systems and rules are set up for this transfer. The speed with which digital data can be transferred is, for example, a crucial ingredient to online communication. Digital electronic data afford the building of *networks*, which means that new group formations can occur. They are also *traceable*, which is key not only to communication and networking, but also the reason why any open data transfer can be surveilled, making it possible to capture and store information. Crucially, digital information is made, unmade, and *co-created* by people and machines in different environments (Kaufmann and Jeandesboz, 2017). This means that digital criminology is not the study of society *or* technology, but of socio-technical phenomena. Technologies do not emerge without context. Designing, building, using, even destroying technologies is always a process that involves humans and technologies alike. All technologies—an encrypted network, a platform for policing or sex work, a messaging app, a database or an electronic shackle—have design decisions built into them that are part of shaping how digital practices and dynamics unfold. Humans and technologies are entangled in that they shape one another. Each of them has agency (see Agency by Krasmann). Technologies and their use, then, need to be understood in their *specificity*, that means in the specific contexts in which they appear and take effect.

Crime, victimization and digitalization

Paying attention to agencies and affordances can help us find entry points for studying digital aspects of crime and victimization. Digitalization affects most fields of criminol-

ogy (and if it does not, its absence may also be an interesting aspect to study). Consider how online markets and banking change financial crime and surveillance (see Financial Crime and Surveillance by Amicelle). Electronic gadgets enable new forms of identification, but also ID-theft (see Identity theft by Langford, Svensson, and Wærstad). Synthetic data can be used for enhancing privacy, but also for mis/information practices or the generation of illegal contents (see Synthetic Data and Generative Machine Learning by de Vries). Social media can enable social networks that have a preventive effect on their members, but also propaganda, radicalization and 'networked hate' (see Hate Crime and Networked Hate by Cameron, Stratton, and Powell), violence, vulnerability, or victimization.

Studying digital dimensions of crime is not the same as studying cybercrime. Cybercrime is often used as an umbrella term which includes all offenses either occurring in or being facilitated by an online environment. Research on cybercrime is very established in criminology. Yet, its focus on online phenomena implies that offline offenses fall out of its scope (Cybercrime by Holt and Holt). Digital criminology, as outlined in this handbook, underlines that a study of online crime would take offline, analog, or other aspects that enable criminal practice into account. What is more, a strict definition of cybercrime would relate to crime only. However, since digitalization is a process of constant change, definitions as to what counts as crime, what is criminalized and in need of regulation are under constant development, too. When using 'digitalization' instead of 'cybercrime' as a vantage point we can take account of these dynamics and ambiguities.

New forms of online vulnerabilities (see Vulnerability by Ranchordas and Beck) emerge hand in hand with new forms of online victimization (see Victimization by Walklate). While not all examples of victimization are an offense, they may become an offense in need of legal regulation. The same is true for online abuse. Not only do practices such as sexting or revenge pornography challenge traditional cultural conceptions of abuse especially when it comes to age, gender, and the status of the 'deserving' victim (see Abuse by McAlinden). But much of such online behavior still has to be understood and established as criminal offense before it is integrated into law. That is to say, digitalization enables versions or varieties of crimes that first have to be identified as those. For example, as more and more administrative fields are digitalized, new forms of ID-theft occur. The above underlines the importance to study how digitalization alters criminalization processes.

Even when a certain digital practice is established as an offense, it is not necessarily clear who will be treated or targeted as the offender: is the individual or are entire platforms and their owners liable? It is thus crucial for criminologists to take into account how digital and online devices influence classic criminological themes of criminalization and liability. At what point is the sharing of sexualized content a form of abuse, who is the offender and what is the role of digital technologies? When is hacking a creative and progressive practice and at what point does it turn into an offense (see Hacking by Wall)? How does the migration of drug markets to the darknet create both positive and negative effects on drug consumption? How can law-making take ac-

count of the two-sidedness of the darknet as it provides encryption and safety from surveillance on the one hand, and a haven for criminal activity on the other (see Darknet by Tzanetakis)? How are control and care entangled in the design of robots, and (when) can robots be considered victims of crimes and violence (see Robots by Lintvedt and Sandvik)?

While many of these issues have been present in law-making for a long time, digital technologies create new practices and dilemmas, because they are characterized by a different set of affordances that allow for a variety of usages. Online digilantism, for example, is the use of the internet to act on perceived offenders without legal authority (see Digilantism by Trottier). An example are social media groups that take initiative to report what they consider as offensive or confront the alleged offender themselves. Digilantism is different from vigilantism, its offline counterpart, because it is mediated by networked technologies that allow their campaigns to 'go viral.' When is digilantism, then, a positive form of social online engagement and at what point does it turn into networked hate with a potential for offline confrontation and violence? And how does the digital environment enable or disable this?

Using digitalization as a vantage point for empirical studies is thus also a way of acknowledging the complexities of phenomena. One example is sex work, where the internet, smart phones, and cameras play an increasingly central role. By going online, a new market for sex work has been created and new powerful actors, for example platform owners, emerge (see Platforms by Egbert). These can act as both protectors or gatekeepers for sex workers. Digitalization generates new possibilities for sex workers, such as audiences and fans, but also vulnerabilities such as being recorded without consent, or they face risks of being exploited by platform owners (see Sex Work by Rand).

Crime control and digitalization

Electronic digital data afford activities of measuring, calculation, and tracing, which means that they also afford new means of crime control. All three are key to the logic of surveillance, of collecting information about individuals, groups, and behavior, and of categorizing this information into risks and predictions. While surveillance has always existed in analog and non-digital forms (see Surveillance by Lyon), it has recently been joined by concepts of dataveillance (Clarke, 1988), capture (Agre, 1994), surveillant assemblages, and data doubles (Haggerty and Ericson, 2000). All of these concepts can be questioned and developed further. What their emergence indicates, however, is that the exponential rise of electronic data has led to an exponential rise of surveillance. Such growing volumes of anything from metadata to free text (e. g., in messages) are in need of evermore sophisticated data processing programs. Algorithms can be trained with more, or less, human interaction, the latter of which we find in machine learning or Artificial Intelligence (AI) models. AI is not new, but evermore powerful computers can analyze large amounts of both structured data (i. e., data organized in

categories) and unstructured data (un- or less organized data). All of these developments have also increased the use of AI in crime control (see Artificial Intelligence by Van Brakel).

Police intelligence, for example, has a long history, but technological advancements are here of particular relevance due to the central role that information plays in intelligence practices. New trends and surveillance solutions enhance collecting, storing, analyzing, and presenting data and information (see Intelligence by Gundhus and Lundgaard). These developments also link intelligence analysis to other digital technologies, such as prediction software and data integration platforms that are adopted across police institutions, including patrol. Symptomatic of this shift is the rise of strategies such as predictive policing and precision policing, as mentioned above. Overall, the volumes and combinations of datasets, advances in predictive analytics and data mining, as well as competitive markets in security technology, have all congealed to mobilize an intensive datafication of police work that continues to accelerate (see Policing by Wilson). The growth, impact, and meaning of facial recognition technology in policing is another example that represents a dramatic shift in police surveillance capability (see Facial Recognition by Fussey). Here, public institutions are increasingly dependent on private technology providers whose range of products tend to cover much more than law enforcement applications. As a consequence, new meeting points between different public and private surveillance practices emerge.

The digitalization of crime control extends to jurisprudence. Courts used to be synonymous with central, imposing buildings where proceedings took place in the presence of the parties and before a judge. Today, courts are moving online and employ AI for decision-making (see Online Courts by Mentovich and Einy). While these changes may render proceedings more efficient, they are also met with issues of representation and unequal access to digital infrastructures. Sentencing algorithms, too, may provide efficiency and structure, but also perform hidden and obvious forms of discrimination (see Sentencing and Risk Assessment Algorithms by Ugwudike). A key issue is thus that digitalization entrenches unjust systems and discriminatory practices in legal domains, which introduces new power dynamics. These dynamics call for new concepts of justice, as for example captured in the term *data justice* (see Data Justice by Redden)

Punishment, too, is being digitalized, where surveillance plays a key role. An example that illustrates the transformative power of electronic surveillance may be the footcuff, originally an iron ball connected to a prisoner's foot, used to prevent escape. The footcuff is something that assists in, but is not per se surveillance. When it comes to prison surveillance, Jeremy Bentham became famous for his panopticon. Its architecture allows guards to watch inmates at any point in time without the inmates knowing when the guard is watching. Today, the footcuff and the panopticon are combined and built into ankle bracelets that carry sensors to remote-trace convicts (see Punishment by Lunde and Scharff Smith). The advantages, challenges but also promises and desires related to digital prisons will have to be documented and gauged in ongoing assessments.

Indeed, the digitalization of crime control needs to be understood in terms of its expectations and consequences. And the expectations that law enforcement has towards *big data* are big (see Big Data by Završnik). Terms such as the 'data deluge' (Bevan, 2015) and 'data tsunamis' (Rubinstein, 2013) suggest that data are liquid and can take any form. The shape or the patterns that (we make) data reveal form the basis for taking action. For that reason, patterns are adopted all across law enforcement. As illustrated above, patterns influence policing (where to focus police attention), intelligence (identifying suspicious patterns), sentencing (identifying those likely to reoffend)—and much more.

Association is here a key analytic practice, which is also used to process analog information (cf. Kaufmann, 2023). To associate is to join, to make a connection "in an interest, object, employment or purpose" (Harper, n.d.), which also could be done on paper or with simple calculations. With the rise of digital information, however, association has shifted in terms of reach, quality, and scale. Very large datasets can no longer be managed and analyzed by humans alone, which is why computation and algorithms have become so important. Algorithms associate different datasets with each other (see Kaufmann, 2023). The most common approach of associating different datasets with each other follows a Boolean logic (Kitchin, 2016), named after the mathematician George Boole. We know them as if-then rules, that is: when *if* is true, *then* is executed. Here, patterns are identified via correlative logics. Another type of association is to generate patterns as we find in so-called 'self-learning' algorithms and large language models like Chat GPT. Association has become a central aspect of surveillance. It is critical to any kind of categorization, sorting, and profiling that we experience on an everyday basis in public management, including law enforcement, health policy, welfare schemes, migration, and border control. All of them are key areas of societal organization, where categories and patterns are expected to produce actionable knowledge (see Categorization and Sorting by Franko).

The implications of the molecularization of society, as Nikolas Rose observes them, are also reflected in digitalization, producing a shift in law enforcement: away from a *deep ontology* aimed at studying causalities, towards a *flat ontology* concerned with circulations and correlations (Rose, 2000). That is to say, thinking of society at a molecular and digitalized level places the focus on management, correlations, and surfaces rather than depth and causalities. The rising confidence in patterns as a base for managing societal relations is expressive of this flat ontology. The propensity of digital data to aggregate, the hunger for evermore-complete datasets and their analysis favor patterns, profiles, and categories over individuality. The growth of databases (see Databases by Bellanova) and the need for automation to analyze them (see Automation by Mann), too, are symptomatic of flat ontologies. They replace the attempt to capture "a set of circumstances in the world" (Amoore, 2011: 32) with the logic of the *derivative:* "the data derivative is exposed to the underlying data without collecting them, created across the gaps and absences, in the interstitial spaces of inference and expansion" (Amoore, 2011: 33). The derivative does not reflect 'circumstances in the world', but it is an analytic device to manage, amongst other things, offenders, crime, and pathology.

One ambition is here to analyze large datasets in order to enhance precision and to arrive at the particular. Today, this even involves the generation of synthetic data in order to increase accuracy (see Synthetic Data and Generative Machine Learning by de Vries). However, the particular slips away in the process of creating actionable knowledge in the form of a data derivative, a pattern, a type (Hopman, 2023). Hence, increasing differentiation and larger datasets do not lead us to the particular, but only to its increasingly differentiated type. How such derivatives, patterns, and types circulate in specific criminological domains, how they change crime and crime control is yet another central aspect of digital criminology. These rationalities are entrenched with a range of challenges and power-dynamics, which underlines the many ways in which digitalization is political.

The politics of digitalization

Digitalization requires investments. *Budgetary policy* prioritizes certain forms of digitalization over others. This is a field that becomes relevant to criminologists when they study law enforcement institutions, where tech adoption, institutional culture, and budget decisions define digitalization processes. The costs of digitalization also affect related domains through knock-on effects. Labor markets and work cultures are classically impacted by the development of technologies. Here, the thrive for efficiency and effectiveness is also challenged by worries about a compromise of competence and dispensation amongst personnel, something that criminologists have also studied in relation to the digitalization of police work or court rooms (Ratcliffe et al., 2020).

But there are also more overarching *economic dimensions* to digitalization. Most digital infrastructures are owned by private companies and public–private partnerships have long histories in law enforcement. And yet, the capitalist role of big tech companies and related market economies increasingly define the ways in which technologies are used in law enforcement. Whether in punishment and sentencing, police and forensic work—providers of technological solutions are normally private. Commercial interests of selling and developing products render both private users and public institutions into customers, where knowledge-making and expertise is co-produced by public and private actors, if it is not outsourced entirely (see Privatization by Lomell). When law enforcement becomes increasingly digitalized, it is indispensable that criminologists take account of the role that private companies play in prosecution, surveillance, and data work in organizations. While some digital solutions do not use customer data for training and development, many private technologies are data-hungry. Not only does that turn user data into the prime capital, but it also places surveillance at the base of technologies' functioning (Zuboff, 2019).

In many ways, however, data have also become less available or traceable, which is where *black boxes* or *blackboxing* comes into play (Latour, 1999; Pasquale, 2015). The changing relationship between the public and the private is a central aspect here, too. Due to the collaborations of public and private actors, public data are not neces-

sarily open data in the sense that they are publicly available. In the history of information much data owned by public institutions was accessible to specific public entities only, e.g., the police. However, with the rise of electronic infrastructures, access becomes a key issue: a lot of information is owned and managed by private companies that enable and restrict data access.

For individuals it has become impossible to own or even access electronic data about themselves. One reason for that is the complexity of digitalization as digital traces of individuals spread across different services and devices. Another one is that data are integrated into bulk analyses, traded, re-used, and appropriated as capital by providers of services which makes it impossible for individuals to own or even trace information. What is more, accessing electronic data requires know-how and infrastructure, which becomes a challenge for individuals, public institutions, and even companies depending on the type of data to be accessed. Here, new vulnerabilities and vulnerable populations emerge. A second issue that complicates access is the changing capacities and practices of calculation. Data analysis has become complex, surpassing human ability to follow. What is more, in many cases access to datasets and knowledge about calculative processes are business secrets, a black box by choice and a result of privatization. These dynamics of in/visibility impact discretion: decisions are co-shaped by algorithmic logics and (semi-)privatized institutions, something that is particularly sensitive in the field of security, crime control, and law enforcement.

Due to their mathematic form, it is seductive to think of computers and algorithms as neutral instruments (Goffey, 2008: 16). However, the initial design and training of algorithms are the result of socio-technical interactions, which necessarily creates machinic *bias and discrimination*, whether positive or negative (see Bias by Oswald and Paul). Bias, then, is everywhere. Even with the increase in data and computation technologies, data analysis has not become more neutral. Current debates about the type of databases used or the parameters of algorithms illustrate that computation is and will be a socio-technical issue. Claudia Aradau offers the analytic concept of *error* as a force for development. It was the errors in the early (anthropo)metric projects that led criminologists to continue to engage with digital systems, including today's electronic solutions (see Error by Aradau). Error is also related to failure, a term that Shoshana Magnet and Ravida Din use to describe the negative bias and the discriminatory nature of today's surveillance systems (see Biometric Failure by Din and Magnet). This can include failures to identify specific skin colors, the exclusion of people with disabilities from digitalization, forms of categorization that are racist and produce disproportional or unfair effects, as well as algorithms that do not pick up on certain forms of victimization. Data have become more than big, however, in tandem with the challenges of skewed data collection. Here, the discrete nature of digital data also contributes to the issue of discrimination. Digital, as mentioned above, refers to measurement in discrete units. In its electronic format, too, digital data are expressed in ones and zeros. The inability to capture anything on a continuum—or to put it differently: the need for

categorization—necessarily leads to types, profiles, and groups and the risk of creating discriminatory categorizations is high.

Catch-phrases such as FATE, which stands for Fairness, Accountability, Transparency, and Ethics (Shin and Park, 2019), are applauded vantage points for the *regulation of big tech*, but notoriously hard to implement. The issue of regulation brings us back to the point that large databases and proprietary software are key to many private companies' business models, protecting businesses from having to release their algorithms or publicizing their databases. This complicates legal regulation. In fact, regulation tends to be privatized as terms and conditions are written by tech owners. Companies effectively become the regulators of digital information flows and digital behavior, increasingly appropriating domains originally governed by public law and criminal justice agents. Lawmakers are then left with limited options for contents to regulate. Effectively regulating such contents would also require streamlined international laws in order to be effective. Such laws would also require all companies to enact transparency in a way that actually enables an understanding and the regulation of technologies. However, the fact that solutions are increasingly complex and complicated to understand—even for their owners—does not make the regulation of technologies any easier. The European AI Act (European Commission, 2021), for example, places the main emphasis not on regulating technology development per se, but on risks related to technology usage. These risk categories would range from minimal to unacceptable risks, where the "biometric identification and categorisation of people" (European Parliament, 2023), for example, would count as unacceptable. However, not only is this risk category so broad that many technologies already in use would be considered unacceptable, but a prohibition of their use would also hamper market competition. While both of these effects can be positive, it remains to be seen how regulation can and will be implemented in practice and whether Europe is able to attenuate the powerful influence of Silicon Valley and equally powerful tech hubs in Africa and Asia.

Regulating the use of technology for surveillance purposes, meaning limiting *privacy intrusion* and defining the threshold to suitable, necessary, and proportional use of surveillance, is yet another issue that has been subject to a long-standing debate. The General Data Protection Regulation (GDPR) implemented by the EU is here often cited as the highest standard privacy regulation in the world (European Parliament, 2016). While it does prevent some companies from operating in Europe, the use of surveillance for security purposes is the argument that creates a loophole in any privacy regulation. Any of these regulatory aspects are important to navigate and study when criminologists assess the use of technology in their field of expertise (see Privacy and Data Protection by Bygrave).

Studying digital phenomena

Studying digital technologies, practices, and environments does not only require analytic concepts, but also suitable methods. Generating insight into digital practices

also invites or requires researchers to navigate technologies as research tools. Surveillance studies and digital sociology have here paved the way for adopting new methods and reflecting about the ways in which digital technologies are part of making criminological knowledge. Deborah Lupton, for example, traced how many traditional methods in sociology have become digitalized, such as interviews, surveys, or observation (2014). When studying documents and other types of texts, Rogers distinguishes between 'digitised data objects,' those that existed as film, photo, audio, text etc. before digitalization, and those that are 'native' to the electronic digital contexts (2014). Though intuitively one would place the analytic focus on databases, software, or AI-generated contents to understand digitalization, there is value, as this chapter argues, to understand which non-digital, low-tech, analog, or offline technologies are part of such 'native' objects (see Low-Tech by Vestad). At the same time, it is of analytic importance to take account of the specific properties of electronic digital objects to understand how and why they work in the making of criminological knowledge. Here, the fields of netnography (focusing on online environments) and digital ethnography (including any digital tool) open different doors to understand digital cultures and phenomena (see Online Ethnography by Gibbs and Hall). Digital criminology, then, is not just a study of humans that use technologies, but also a study of digital devices and online phenomena: how do we make a digital object speak? Adams and Thompson suggest gathering anecdotes about digital objects, following actors, understanding affordances or 'invitational qualities' of digital technologies, studying breakdowns, translations, and passages, that is studying how technologies become what they are (see Interviews with Digital Objects by Adams and Thompson). In such contexts, the laboratory is also an important but largely understudied site in criminology. Labs play an important role in crime and crime control, but also in the development of the discipline and its scholars. Laboratories do not just produce new technologies, practices, and knowledge. They also produce 'new types of people,' that is subjectivities expressive of ongoing societal and professional digitalization (Schmidgen, 2021; see Labs by Mazzilli Daechsel).

Understanding how digital objects are part of creating criminological knowledge is also key when choosing a specific digital technology for establishing access to a group, or for conducting interviews. For example, while one could make offline, face-to-face interviews with drug consumers, the relative anonymity of encrypted sites can be an alternative that allows for different interview dynamics, which can lead to different or new insights. These interviews can be held on gaming software and other encrypted channels, or texting apps—just to name a few (see App-Based Textual Interviews by Bakken). Sex work, too, may be understood differently with different methods. While research on sex work has a long and important history of studying offline environments, sex work itself has also moved online. This means that researchers should also pay attention to chats and forums for understanding online groups and practices of within their specific field (see Researching Online Forums by Šupa). Indeed, seeking access to relevant fora or social media is crucial when conducting research on phenomena that are regarded as digitally native, such as online radicalization. When doing so, navigating the balance of public and private space, or even using one's own accounts

for such research projects requires careful planning (see Recruitment via Social Media by Andersen). An alternative way of approaching online radicalization could also be from the side of those who seek to regulate it, their online presence, and their use of tools for the detection and analysis of user patterns.

A tool that is suitable for both qualitative and quantitative projects is the net crawler. They are particularly useful if the aim is to collect a lot of structured information from the internet, that is content data presented in the same patterns, i. e., a chatroom with date, time, a line for a heading, and a content box. A crawler is a program that can be used to automatically collect or 'scrape' this content. Often, however, these are large datasets that require structured storage and analysis with yet different software solutions. Not only is it crucial to be aware of the variations different software solutions can produce in analyses, but it is also key to reflect about the ethics and the invasiveness of crawling data that is not produced for the purpose of doing research. As with researching online forums, such research requires careful reflection about the relative privacy and personal character of information shared online despite it being publicly available. Alternatively, it is also an option to look at services that have already conducted statistical analyses, such as Google Trends or n-grams, for example for checking the use of specific terms over time. It is, however, important to reflect about the limits of this pre-given information and the ethics of using big tech services for doing research. There are many ways of using automation and digital tools for doing research. Some designs, for example, also implement experiments that expose people to robots. Such research designs require careful and ongoing ethics monitoring (see Ethics by Markham).

There are plenty of ways of adopting digital objects and methods into criminological research: by using simple digital devices to record conversations, by coding pictures or videos, by analyzing algorithms, by studying or building databases, by using social media actively, by using the encrypted net or 'darknet' as a site for research, by following discussion forums, capturing websites, collecting tweets/Xs, or following digital devices around in everyday practices. Art, too, is an entry point to knowledge production and reflections. Here, art projects can embrace speculation more freely than classic research methods. Through this, art can create new insights, but also prompt commentary and critique (see Art as Method by Dewey-Hagborg).

What is key to all the above-mentioned methods and digital devices for knowledge production is to consider their ethical implications: Why should it be fair to use data for research that are produced by others in a non-academic context? Is my approach extractivist, i. e., do I harvest or mine data in an unfair or destructive fashion? Is the method I choose safe for everyone participating in research, including myself? How do I protect data and when do I cross the line into private spheres? Do the tools I use for analysis do the phenomenon I study justice? In many ways, these questions apply to analog and digital methods alike. But it is their 'digitality' that needs to be a point of reflection, that is: How do the properties of electronic digital data and environments change methods, practicalities, and ethics? A thorough understanding of the technologies we use to do research is key to reflect about the ways in which

they shape access, participation, interactions, communication patterns, research data. Good knowledge of one's digital research tool is key to assess their advantages and limits—and most important—reflect about one's own co-creative role in the research process (see Accessing Online Communities by Kaufmann). Technologies are not only part of our attempts to understand social practices and phenomena, but they also shape the knowledge we create about them.

Openings

The ambition of digital criminology is to establish itself "within the discipline, not as a sub-discipline" (Powell et al., 2018: 190). Digitalization is a phenomenon that cuts across all criminological fields, affecting criminalization, crime, and crime control alike. Digitalization is not a new phenomenon. The original meaning of the word *digital* relates to measuring, counting, and calculation. These were equally relevant for the metric and statistical ambitions of early 20th-century criminology as they are today when complex computing technologies continue to re-shape societies. Hence, we invite readers to examine the continuities and changes, as well as the materialities and socio-technical activities that characterize digitalization. We invite readers to help characterizing 'the digital' further by studying processes of digitalization in their specific contexts, moving beyond simple online/offline, analog/electronic, high/low-tech distinctions. Questioning linear accounts of digitalization, ambiguating categorizations, and transgressing epistemological borders is what digital criminology can contribute to the study of technology, crime, and crime control (see Borders and Border Control by Jeandesboz).

This book should be read as a real handbook, a guide for crafting knowledge, in that it provides a glossary with concepts, tools, themes, and methods that equip readers with the key definitions of a term and suitable further readings. The book is edited to inspire. It encourages readers to combine analytic devices with methods and themes that are relevant to their area of interest. While it could seem like some entries relate to either crime or crime control, method or theory, many chapters touch upon several cross-cutting aspects, which is why this handbook's chapters or terms are presented in an alphabetic list rather than in sections. We see value in finding the ambiguities in both the 'digital' and the 'crime' in 'digital criminology' as they vary across different fields and jurisdictions.

Since digital criminology relates to fast-moving, diverse, and dynamic phenomena, handbooks are necessarily incomplete; neither do all authors fully adopt each other's analyses. We thus expect readers to question terms, develop them further and add new ones. What is more, we also want to push readers to consider how their own findings can challenge and change the politics and dynamics of digitalization. This can be done by complicating easy distinctions between crime and crime control, or by providing pathways for tackling discrimination, exploitation, and surveillance creeps, for avoiding victimization, reducing vulnerabilities and injustices that an emerge in tandem with digitalization.

References

Agre, P. E. (1994). Surveillance and capture: Two models of privacy. *The Information Society*, 10(2), 101 – 127.

Amoore, L. (2011). Data derivatives: On the emergence of a security risk calculus for our times. *Theory, Culture & Society*, 28(6), 24 – 43. https://doi.org/10.1177/0263276411417430.

Basaglia, F., & Ongaro Basaglia, F. (1971). L*a maggioranza deviante.* Turin: Einaudi.

Bevan, A. (2015). The data deluge. *Antiquity*, 89(348), 1473 – 1484. doi:10.15184/aqy.2015.102

Burrows, R. (2009). Afterword: Urban informatics and social ontology. In M. Foth, *Handbook of Research on Urban Informatics: The Practice and Promise of the Realtime City* (pp. 450 – 454). Hershey: IGI Global.

Clarke, R. (1988) Information technology and dataveillance. *Communications of the ACM*, 31(5), 498 – 512.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44(4), 588 – 608.

Cornish, D. B., & Clarke, R. V. (1986). *The Reasoning Criminal: Rational Choice Perspectives on Offending.* New York: Springer-Verlag.

European Commission. (2021). Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts. COM/2021/206 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206 (Accessed 16 February 2024)

European Parliament. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). https://eur-lex.europa.eu/eli/reg/2016/679/2016-05-04 (Accessed 16 February 2024)

European Parliament. (2023). EU AI Act: First regulation on artificial intelligence. https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence (Accessed 16 February 2024)

Floridi, L. (2010). *Information. A Very Short Introduction.* Oxford: Oxford University Press.

Gibson, J. J. (1979). *The Ecological Approach to Visual Perception.* Boston: Houghton Mifflin.

Gibson, M., & Rafter, N. (2006). Editors' introduction. In C. Lombroso (ed.), *Criminal Man* (pp. 1 – 36). Durham, NC: Duke University Press.

Goffey, A. (2008). Algorithm. In M. Fuller (ed.), *Software Studies – A Lexicon* (pp. 15 – 20). Cambridge, MA: MIT Press.

Hacking, I. (1990). *The Taming of Chance.* Cambridge: Cambridge University Press.

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

Harper, D. (n.d.). Associate. Online Etymology Dictionary, https://www.etymonline.com/word/associate#etymonline_v_17972 (Accessed 24 November 2022)

Hopman, R. (2023). The face as folded object: Race and the problems with 'progress' in forensic DNA phenotyping. *Social Studies of Science*, 53(6), 869 – 890. https://doi.org/10.1177/03063127211035562.

Johnson-Groh, M. (2023). *Achieving More with Less: Optimizing Efficiency in Supercomputing.* Simons Foundation. https://www.simonsfoundation.org/2023/02/22/achieving-more-with-less-optimizing-efficiency-in-supercomputing/ (Accessed 16 February 2024)

Kaufmann, M. (2023). *Making Information Matter. Understanding Surveillance and Making a Difference.* Bristol: Bristol University Press.

Kaufmann, M., & Jeandesboz, J. (2017). Politics and 'the digital': From singularity to specificity. *European Journal of Social Theory*, 20(3), 309 – 328.

Kitchin, R. (2016). Thinking critically about and researching algorithms. *Information, Communication & Society*, 20(1), 14 – 29.

Latour, B. (1999). *Pandora's Hope: Essays on the Reality of Science Studies.* Cambridge, MA: Harvard University Press.

Lomell, H. M. (2010). The politics of numbers: Crime statistics as a source of knowledge and a tool of governance. In S. G. Shoham, P. Knepper, & M. Kett (eds.), *International Handbook of Criminology* (pp. 117 – 152). Boca Raton: CRC Press.

Lomell, H. M. (2011). Making sense of numbers: The presentation of crime statistics in the Oslo police annual reports 1950 – 2008. In A. R. Sætnan, H. M. Lomell, & S. Hammer (eds.), *The Mutual Construction of Statistics and Society* (pp. 191 – 206). New York: Routledge.

Lupton, D. (2014). *Digital Sociology.* London: Routledge.

Maurutto, P., & Hannah-Moffat, K. (2006). Assembling risk and the restructuring of penal control. *The British Journal of Criminology*, 46(3), 438 – 454. https://doi.org/10.1093/bjc/azi073

Montaldo, S. (2018). Lombroso: The myth, the history. *Crime, History and Societies*, 22(2), 31 – 61.

Pasquale, F. (2015). *The Black Box Society: The Secret Algorithms that Control Money and Information.* Cambridge, MA and London: Harvard University Press.

Peeters, R. (2013). *The Preventive Gaze. How Prevention Transforms Our Understanding of the State.* The Hague: Eleven International Publishing.

Powell, A., Stratton, G., & Cameron, R. (2018). *Digital Criminology.* Abingdon: Routledge.

Quetelet, A. ([1842] 1996). On the development of the propensity to crime. In E. McLaughlin & J. Muncie (eds.), *Criminological Perspectives. Essential Readings* (pp. 23 – 39). London: SAGE Publications.

Ratcliffe, J., Taylor, R. B., & Fisher, R. (2020). Conflicts and congruencies between predictive policing and the patrol officer's craft. *Policing and Society*, 30(6), 639 – 655. DOI: 10.1080/10439463.2019.1577844

Rogers, R. (2014). *Digital Methods.* Cambridge, MA: The MIT Press.

Rose, N. (2000). The biology of culpability: Pathological identity and crime control in a biological culture. *Theoretical Criminology*, 4(1), 5 – 34.

Rubinstein, I. (2013). Big Data: The end of privacy or a new beginning? *International Data Privacy Law*, 3(2), 74 – 87. https://doi.org/10.1093/idpl/ips036

Schmidgen, H. (2021). The laboratory. *Encyclopedia of the History of Science.* doi: 10.34758/sz06-t975

Shaw, C. R., & McKay, H. D. (1972). *Juvenile Delinquency and Urban Areas.* Chicago: University of Chicago Press.

Shin, D., & Park, Y. J. (2019). Role of fairness, accountability, and transparency in algorithmic affordance. *Computers in Human Behavior*, 98, 277 – 284.

Shults, Chief J. F. (2022). *Precision policing: The next law enforcement era.* https://www.police1.com/investigations/articles/precision-policing-the-next-law-enforcement-era-q4cwlki2hY9DyJTY/ (Accessed 16 February 2024)

Smith, D. (2015) *Google Chairman: 'The Internet Will Disappear'.* Business Insider. https://www.businessinsider.com/google-chief-eric-schmidt-the-internet-will-disappear-2015-1?op=1&r=US&IR=T (Accessed 16 February 2024)

Star, S. L., & Griesemer, J. R. (1989). Institutional ecology, 'translations' and boundary objects: Amateurs and professionals in Berkeley's Museum of Vertebrate Zoology, 1907 – 39. *Social Studies of Science*, 19(3), 387 – 420.

Thrasher, F. M. ([1936] 2013). *The Gang. A Study of 1,313 Gangs in Chicago.* Chicago: The University of Chicago Press.

Thrift, N. (2004). Remembering the technological unconscious by foregrounding knowledges of position. *Environment and Planning D: Society and Space*, 22(1), 175 – 190.

Zedner, L. (2007). Pre-crime and post-criminology? *Theoretical Criminology*, 11(2), 261 – 281.

Zuboff, S. (2019). *The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power.* London: Profile Books.