Fourteenth United Nations Congress on Crime Prevention and Criminal Justice

15 February 2021

English only

Kyoto, Japan, 7–12 March 2021

Item 6 of the provisional agenda[*]
International cooperation and technical assistance to prevent and address all forms of crime:
(a) Terrorism in all its forms and manifestations;
(b) New and emerging forms of crime

Background documents received from individual experts[**]

AI-Algorithm-Big Data, Predictive Criminal Justice and Hyper Crime/Social Control: Surveillance Capitalism after 'Singularity' and Prospects of Informational Civilization

Prepared by Noriyoshi Takemura

[*] A/CONF.234/1/Rev.1.

[**] The designations employed, the presentation of material and the views expressed in the present paper do not necessarily reflect the views of the United Nations Secretariat and do not imply the expression of any opinion whatsoever concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

The 14th United Nations Congress on
Crime Prevention and Criminal Justice
Kyoto, March 7-12, 2021

AI-Algorithm-Big Data, Predictive Criminal Justice and Hyper Crime/Social Control: Surveillance Capitalism after 'Singularity' and Prospects of Informational Civilization

Background document from individual expert
Prepared by Noriyoshi Takemura

April 2020

Noriyoshi Takemura

Professor of Criminal Law and Criminology
Toin University of Yokohama, Japan

AI-Algorithm-Big Data, Predictive Criminal Justice and Hyper Crime/Social Control: Surveillance Capitalism after ‘Singularity’ and Prospects of Informational Civilization

Abstract

Current real society is surprisingly resembling a dark society in the near future which scientific fictions frequently draw. In famous scientific fiction “Minority Report” a policeman, who works at ‘department of crime prevention’ in Washington D.C., arrests would-be criminals based on pre-crime logic. Today police can use many kinds of data and technologies which GAFA etc. offer. In recent years private companies are concerned in activities of solving criminal cases, crime prevention and information compilation by authorities. In May 2018 human rights associations including ACLC sent Amazon a letter in which they asked to stop selling police the pictures processing system called Recognition. This system has a possibility to be a serious threat to communities of colored people and immigrants.

In this context it is significant to consider dystopian dark sides which a mass surveillance with many kinds of technologies may have. Recently, using big data, Los Angeles city police is developing a model which predicts crime would happen places. A research found that the way of using big data has radically changed a quality of police activities. Main police activities are prospecting would happen places with mass surveillance rather than responding crimes after happening crimes. This model has a risk to keep a person under surveillance who had no contact with police before because it analyzes mixing many kinds of data sources. With advancing current situation and AI and IT have developed in the future, after the ‘singularity’ comes, what will happen around human beings? Human being might be an unification of data and physical body, and the former will be more significant than the latter. In the network, co-extensivity may replace simple co-presence. Actants are simultaneously informational and organic entities in the deepest sense, technology co-extensive with the human sensorium. In other contexts, human being may be rendered as information actant. We need develop a ‘critical analysis of AI-Algorithm-Big Data using predictive hyper crime control’, facing the surveillance regime of state-company-citizen Trinity, which advances under the slogan of ‘security and safety’ from super to hyper, and under which make possible all kinds of social control based on the principle surveillance society, ‘big data’.

In this research, concerning a ‘predictive hyper crime control’, following problems are cleared and deliberated: AI-Algorithm-Big Data and predictive policing; automated criminal justice system and hyper crime control; surveillance capitalism after singularity and prospects of information civilization.

1. Introduction

Humans have become data-producing machines. Every Google search, credit card purchase, social media interaction, and doctor’s visit leave traces of information about us, where we have been, who we have interacted with, and what we like. What’s more, advertisers, data brokers, and government agencies can collect and analyze the digital breadcrumbs we leave behind as we go about our day.

While data-driven technologies may be used for the benefit of individuals and society as a whole, they run an equal risk of entrenching discrimination and exacerbating various forms of inequality. The realm of criminal justice is no exception: big data has both the potential to infuse fairness into the administration of justice, and, more worryingly, expedite the reproduction of existing biases.

Whether we like it or not, big data and algorithmic decision-making have become embedded within processes of justice administration around the world. These predictive technologies are appealing because they claim to make justice a speedier, more egalitarian affair. They take complicated and potentially-biased discretionary decisions – such as who to police and who to assess as ‘higher-risk offenders’ - and reduce these decisions to scores, numbers, or dots on a map.

When police relies on big data and predictive analytics, however, their policing becomes more proactive, sometimes aggressively so. Black offenders are more likely to get higher risk scores, which suggest to judges a higher likelihood of reoffending. As a result, these predictive technologies give judges the algorithm-derived permission to treat Black offenders more harshly than others. If the data that criminal justice actors collect and feed into their databases are biased, the results of the predictive analysis using these data will be biased, too. Predictive justice technologies are at high risk of simply reproducing the biases and partialities that already operate in the criminal justice system. The extent to which predictive justice technologies actually reduce, prevent, or anticipate crime is presently unknown.

Big data, predictive software, and risk assessment algorithms have already significantly shifted the criminal justice landscape. These seemingly handy pieces of technology have the capacity to expedite and streamline the work of criminal justice actors, but may do so at the expense of those entering or already entrenched in the justice system. We should maintain a healthy skepticism about the use of big data and algorithmic decision-making, which are only likely to grow more ubiquitous as we head forth into an increasingly technologized future.

2. AI-Algorithm-Big Data and 'Predictive Policing'

2.1 Turning the Crime Tide with Predictive Policing

Although AI is a new concept for the law enforcement community and there are gaps in expertise, McCarthy mentions, many national agencies are already actively exploring the application of AI to enhance crime prevention and control. Perhaps one of the most tantalizing and controversial applications of AI for law enforcement is what is known as 'predictive policing' – the prediction of potential criminal activity before it occurs.

In spite of the technical complexity of this cutting-edge technology, he continues, the concept is quite well known due to the prominent role it plays in several works of science fiction. Perhaps most famously it featured in Steven Spielberg's 'Minority Report' in which a specialized police department uses visions of precognitive people to prevent crimes and to arrest future offenders before the commission of the act. Unlike 'Minority Report', the real version of predictive policing doesn't involve 'precogs' identifying who will commit a crime. Instead, data collected by police departments about the type, location, date and time of past crimes is fed to and analyzed by AI algorithms to generate a forecast of when, where and what types of crimes are most likely to occur. Using these insights, law enforcement can thus optimize its resources by deploying police when and where they may be most needed (McCarthy).

Although no country has put in place a national predictive policing programme as of yet, he analyzes, predictive policing tools have been developed and deployed in several cities across the globe. For instance, in the United States, the company, Palantir, has developed and tested predictive policing tools in cities such as Chicago, Los Angeles, New Orleans and New York as far back as 2012. Another company, PredPol, has also developed a predictive policing tool that has been deployed in approximately 40 agencies across the United States since 2012. Outside the US, police departments in countries such as China, Denmark, Germany, India, the Netherlands, and the United Kingdom are reported to have tested or deployed predictive policing tools on a local level. This list is certainly not exhaustive and is likely to grow as AI becomes more advanced and law enforcement becomes more familiar with its potential (McCarthy).

McCarthy insists that there is also a lot of interest in exploring advancements in machine vision, such as facial recognition, in connection with predictive policing. This combination could further enhance the capabilities of law enforcement to prevent crimes by enabling them, not only to identify when and where they may be most needed, but also to analyze footage collected through surveillance cameras, body-cameras and drones to identify potential offenders in a crowded space or even predict who may commit a crime based upon facial expressions that might indicate guilt (McCarthy).

There are serious issues below the surface, he continues. At the top of the list is the risk that if the data used to train predictive policing tools comes from biased policing, explicitly or implicitly, then the resulting forecast will also bear this bias. Data bias was the focus of the 2016 ProPublica investigation into an AI tool known as COMPAS, which was used by judges to support decision-making on the likelihood of criminals re-offending. The investigation concluded that the data appeared to be biased against minorities. A similar bias in a predictive policing tool could, for instance, change how law enforcement sees the communities they patrol and influence important decisions such as whether to make arrests or use force. Bias may also lead to the over-policing of certain communities, heightening tensions, or, conversely, the under-policing of communities that may actually need law enforcement intervention but do not feel comfortable in alerting the police (McCarthy; INTERPOL and UNICRI; Konikoff and Owusu-Bempah).

2.2 Exploring the Boundaries of Big Data

The government is rightly interested in Big Data, for two reasons: both its potentially positive effects and its potentially negative effects. Van der Sloot et al. analyzes the Big Data techniques for predictive profiling purposes by the police. This might not only have a beneficial effect on the distribution of resources and the effectiveness of policing activities, but also may have an empowering effect on citizens. Many authors, however, also emphasize the potentially negative effects of Big Data. Almost every classic data protection principle is put under pressure in Big Data processes. The same has been observed with regard to the Fair Information Practices and with respect to the fundamental right to privacy. There are also potential problems regarding discrimination and stigmatization, especially when Big Data is used in relation to predictive policing and group profiling. Big Data might have added value when used correctly and appropriately, but it might also have negative effects when applied inadequately. New policies and regulations, therefore, may help to guide the use of Big Data in the right direction (Van der Sloot et al.: 21).

The key question concerns the use of Big Data processes and of techniques such as profiling and data mining. In particular, they continue, the Minister wished to ascertain how these techniques can be used in a transparent manner and how adequate checks and balances can be formulated to allow these techniques to be used safely and carefully. Profiling has been used for a long time but will gain new momentum with the rise of Big Data. Not only the risks of discrimination and stigmatization are pointed out, but also potentially Kafkaesque or 'computer-says-no' situations. The fear is that computer programs and algorithms will increasingly lead their own lives and replace human-led decision-making processes. They suggest that transparency is key here, but that legal obligations curtailing the use of profiling should also be developed. Although such principles are currently already in place in anti-discrimination law, data protection law, human rights law, administrative law, and penal law, in order to properly protect citizens' interests in the Big Data era, they need an overhaul. (Van der Sloot et al.: 22)

Finally, they mention, the Minister wanted to know how the autonomy of citizens can be ensured in Big Data processes. This relates to the question whether a focus on informed consent is still tenable, what possibilities citizens have for effective control over their data, what responsibility citizens have to contribute to the quality of the data in databases, and, more in general, how maintaining quality of information can be guaranteed. First, individuals are often incapable of protecting their own interests through individual rights because they are often unaware of their personal data being gathered and because it will be impossible for them to keep track of every data processing which includes (or might include) their data, to assess whether the data controller abides by the legal standards applicable, and if not, to file a legal complaint. Consequently, individual rights should be supplemented with more general forms of legal protection, such as more and stricter obligations and duties of care for controllers. Second, the interests involved in Big Data processes often transcend individuals and their interests and affect group and societal interests. We need to focus not only on legal rules but also on ethical evaluations and, hence, to consider using Ethical Impact Assessments in addition to Privacy Impact Assessments (Van der Sloot et al.: 23).

2.3 Potential and Disparate Impact of Big Data

Big data's predictive algorithms have the potential to revolutionize the way police investigate crime and the way the courts regulate the police. According to Simmons, for centuries, courts have been crafting legal standards for police officers who were making clinical judgments based on experience and intuition. The imprecision and subjectivity of these legal standards were a necessary evil—they were required given the subjective factors that were used by the police, but their accuracy could not be tested, they made the system less transparent, and they opened the door to vastly inconsistent and frequently discriminatory results. With the rise of big data's predictive algorithms, we have an opportunity to increase the accuracy and the transparency of the way we apply the standards and of the standards themselves, making the system more efficient, fairer, and more open (Simmons 1016-1067).

In order to reap these benefits, he insists, we need to ensure that the predictive algorithms are race neutral and that they take into account individual suspicion. This may require new types of algorithms that are specifically designed for determining reasonable suspicion and probable cause. It will certainly require that the algorithms be transparent, so that reviewing courts can understand what factors the algorithm is using. To be sure, a system of mechanical predictive algorithms and quantified legal standards will not be perfect. It will probably be impossible to scrub all residue of racial discrimination from the existing databases, and police officers and judges will almost certainly make mistakes when trying to use the predictive algorithms as base rates and then adding their own independent observations. And the predictive algorithms themselves will still make mistakes, and thus will not always be as accurate as we would like. But the current system includes the implicit and sometimes explicit biases of police officers and judges; vague standards that can be manipulated by police officers, which are more or less incomprehensible to lay people; and accuracy rates that vary wildly from jurisdiction to jurisdiction. The time has come for courts to embrace the enhanced precision and transparency that big data has to offer (Simmons: 1017).

Predictive policing is rapidly being adopted throughout the country, he analyzes, though it is unclear as of yet whether the technologies even offer any tangible benefit over traditional policing, and there is precious little insight into its discriminatory effects. Machine learning poses new regulatory challenges in many parts of society, but when it comes to police in particular, the track record on discrimination cries out for new forms of oversight and transparency. Police departments must ensure that they are not adopting technology that produces limited benefits while equating 'criminal' with 'black'. If they remain unregulated, predictive policing systems will harden and perpetuate the racial discrimination that pervades the criminal justice system. Unless society recognizes the urgency and acts soon, we will become inured to the toxic discriminatory emissions of predictive policing systems. The narrative pull of 'trusting the data' will hardcode racial discrimination into the technology, making it even harder to eradicate later. Given the history of discriminatory policing, no technology or police practice should ever be adopted without investigating how it impacts minority populations. Society cannot afford to let the allure of new technologies blind people to the systemic inequalities they can perpetuate (Selbst: 193-194; Ferguson; Brundage et al.).

In short, applying 'big data' forecasting to our existing criminal justice practices is not just inadequate, and it also risks cementing the irrational fears and flawed logic of mass incarceration behind a veneer of scientific objectivity. Neither judges nor software can know in advance who will and who won't commit crime. Risk assessments and predictive policing are a case study of how a real-world 'Minority Report' doesn't work.

3. Automated Criminal Justice System and Crime Control

3.1 Future Crime Control: 21st Century Crime Prediction

There are widespread concerns that predictive policing tools could unintentionally exacerbate over-policing of marginal areas and undermine privacy. Aguirre and others mention that it is widely known that algorithms can reproduce existing patterns of discrimination, reinforcing previous errors and biases of programmers and embedded in databases. There are very real ethical questions about the extent to which such tools can influence police to disproportionately surveil marginalized neighborhoods and communities. There are fears that such tools may augment race and age profiling and undermine privacy rights and civil liberties (Aguirre et al.: 8).

There are likewise worries about the ways predictive tools can unfairly target crime offenders and crime victims. For example, they continue, the Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) framework which is used by U.S. courts to determine the likelihood that convicted criminals will commit future crime was found to be biased against minorities. Likewise, the Chicago Police Department was subject to intense scrutiny in 2016 when a study conducted by the Rand Corporation found that individuals estimated to be at highest risk of gun violence were neither "more or less likely to become a victim of a homicide or shooting." The researchers noted that "one potential reason why being placed on the list resulted in an increased chance of being arrested for a shooting is that some officers may have used the list as leads to closing shooting cases" (Aguirre et al.: 9).

In a country with 172 million state-controlled surveillance cameras, they mention, the nation-wide expansion of the initiative can further damage the already battered civil liberties of the Chinese people. The system is said to be imperfect, yielding a large number of false positives when the facial recognition algorithm wrongly identifies a suspect. Experts in law and technology question whether there are due process systems in place to protect citizens from false accusations, and if the false positives are disproportionately skewed toward political dissidents or minority groups (Aguirre et al.: 9).

The accelerated pace and spread of crime and violence prediction tools means that these concerns will only grow in the coming years. Indeed, they explain, new platforms are already being tested that aim to automatically classify gang-related crime, combine social media with criminal history to predict crime, and use artificial intelligence to identify individuals with higher risk profiles of committing terrorist acts. The rapid roll-out of these tools invariably raise complex ethical questions in relation to police action and civil rights (Aguirre et al.: 9).

Policing innovations for agile security also should make use of the interconnection of urban infrastructure including sensors and unstructured data, they insist. Even so, privacy concerns should be paramount in the decision to process such information. Where possible, predictive tools should allow citizens to understand what is inside the 'black box'. While private vendors understandably seek to protect their source code, coupled with their underlying mathematical complexity, this lack of transparency makes it difficult for law enforcement agencies and civil society to understand how the predictions are generated. This can undermine confidence in the tool (Aguirre et al.: 10; O'Neil).

3.2 Automated Justice: Algorithms, Big Data and Criminal Justice Systems

From predictive policing to probation risk scores, the potential uses of big data in criminal justice systems pose serious legal and ethical challenges relating to due process, discrimination, and the presumption of innocence (Collegium Helveticum).

Criminal justice systems are using technological solutions, according to Collegium Helveticum, for instance, to predict future crimes of those applying for bail or those to be sent on a parole. The idea of such 'automated justice' is to vaporize biases, heuristics and to confine fundamentally value-based decisions to 'clean and pure' mathematical reason. There are clear benefits deriving from calculating the risks of misconduct and risk assessments have become relatively standard practice in the criminal systems, e.g. for correctional placement and in the sentencing phase. Such assessment in the sentencing procedure was utilized long before the development of ICT, but algorithms and big data tools for determining prison sentences or for deciding on a parole are relatively newer practices (Collegium Helveticum).

Researchers have shown how relying too heavily on automated calculations of risk may encroach on fundamental liberties. For instance, it explains, in a detailed assessment of the COMPAS recidivism algorithm ProPublica discovered how the system is biased against black individuals. In fact, several scholars have warned how such 'automated governance' can lead to 'social sorting on steroids', and can encroach on fundamental liberties, such as privacy and presumption of innocence and even, ultimately, shake the democratic division of power (Collegium Helveticum; Tréguer).

3.2.1 The age of the algorithmic self: the epistemological evolution and revolution of the effectiveness movement and automated justice

Today, we are witnessing an important technological development in the way risk analyses are performed. Risk assessments are increasingly carried out through algorithm-based big-data analysis. It is argued that this method introduces a new frontier of accuracy, to the extent that it may even eliminate all forms of bias. This development represents a significant step forward in the epistemological transition that started with the effectiveness movement in crime control and administrative criminology. Algorithm-based big-data analysis completes this epistemological evolution or, arguably, revolution. If individual-based theories of crime assumed a pathological self, and neoclassical theories assumed a rational self, big-data analysis brings about an 'algorithmic self'. The old types of self are abandoned; consciousness, reason and clinical diagnoses are replaced with a type of performative knowledge that is a-theoretical, predictive, and non-reflexive. Algorithm-based big-data analysis bypasses consciousness and reason, and offers solutions without concerning itself with the 'path' leading to them ('black box' solutions). In this sense, algorithmic knowledge is a radical break from the types of epistemology that once dominated the modern world, and the knowledge of the world and of the self they produced.

3.2.2 The real-time cop: imaginaries of technology, speed and policing

'Predictive policing' has emerged as the key buzz term of contemporary crime control which extends the promise of anticipating crime prior to its actualization. Marketing materials are replete with strident claims of future crimes that are calculable, knowable and targetable before they transpire. Computer technology from the 1980s onwards intensified such quantification, promising to increase bureaucratic control internally, and with in-car computers igniting the possibility of policing as a seamless information network of real-time transmissions. Predictive policing then, rather than an entirely novel development, is one manifestation of a longer trajectory of police entrancement with technology and quantification, and their potential to facilitate temporal and spatial domination. Moreover, despite the frequent recourse to cultural memes of pre-crime encapsulated in recourse to the fictional example of Minority Report, the objective is not to police the future. Rather, predictive policing envisages a form of policing in real-time – instant policing – that continually suppresses criminal activity at the moment of its unfolding. While acknowledging that operational realities are likely to differ substantially from the promoted vision, the rationalities of the contemporary 'datafication' of policing are explored and linked to wider developments within 'informational capitalism'.

3.2.3 Automated justice: from the rule of law to the 'rule of algorithm'?

The Arnold Foundation algorithm, which is being rolled out in 21 jurisdictions in the USA, uses 1.5 million criminal cases to predict defendants' behavior. Similarly, study of 1.36 million pre-trail detention cases conducted by Stanford University scholars purports that a computer can predict whether a suspect will flee or re-offend better than a human judge. In big data and 'algorithmic' analytics in criminal justice settings, the new language of mathematics is used for blurring contemporary regulatory boundaries, undercutting the safeguards built into regulatory regimes, and abolishing subjectivity and case-specific narratives (O'Neil). The origins of big data in industry and the underlying assumptions, such as "doing more with less," "the numbers speak for themselves" etc., are being transferred to criminal justice system domain where these assumptions have negative consequences for fundamental liberties, such as presumption of innocence and due process of law. With predictive analytics in criminal justice settings, 'big data and algorithms' have changed criminal justice from narrative to database and furthermore towards 'automated decision-making' (Collegium Helveticum).

3.3 'Singularity', Crime and Social Control and its Discontents

The language of big data helps to tear down the walls of criminal procedure rules. Završnik explains that this move towards a system of 'automatic justice' minimizes human agency and undercuts the due process of safeguards built into the traditional criminal justice model. The most far-fetched views contend that big data analytics enables an entirely new epistemological approach to making sense of the world. Such views camouflage big data as an 'objective' and 'pure' knowledge, and neglects the fact that statistics have always been political and served specific political ends. The army of digital workers open to exploitation is used as the means to very specific political ends. There is no 'end of politics' at work here, as the 'reserve army of digital labor' serves the pecuniary interests of the digital industry, which carters to the affluent elite of surveillance society. Digital workers are actually the product being sold on the data market place (Završnik: 4-5).

While being seemingly more objective, knowledge and neutral language, big data, and algorithms carry several caveats, he analyzes. The mathematical predictions and reasoning used in an increasing number of social domains make the study of big data and algorithms inspiring and frightening at the same time. It is not only the idea of the exponentially increasing computer capabilities heading towards the point of 'technological singularity': the hypothesis that the invention of artificial superintelligence will abruptly trigger runaway technological growth (Kurzweil). There are socially destructive consequences of big data and automated decision-making systems already at work und unfolding in surveillance-based capitalist societies in the form of discrimination against the less affluent and less powerful parts of the population (Završnik: 9, 17-18; Harari).

Big data has been granted too much agency and too much power too quickly, he insists. Big data is shifting power relations in several domains, including control and security. Its predictive potentials have become an attractive method of predicting human behavior in too many contexts, including the improvement of fighting against crime. It has been vested with a great deal of power, while at the same time presents as an objective, value-free scientific tool that requires no transparency or auditing and no further explanation. It has become a projection screen for our desire to predict and colonize the future --- to eliminate all the risks to our well-being, but only for those who can afford a data scientist. Big data may be bringing about a revolution that will transform how we live, work and think, but this revolution will not occur because of big data itself, but because of the specific social, cultural, political and economic imperatives in our society that allow such technology to flourish to detriment of other types of knowledge and social practices (Završnik: 18; The Law Society Commission on the Use of Algorithm in the Justice System and The law Society of England and Wales; Bostrom; Clavel; Mainzer; Kurzweil; Hawking; Harari).

In short, AI that is deployed by and for humans can improve the experience of both people consuming information and those producing it. Without people in the loop, we risk losing the web's fundamental humanity. We must keep people at the center of every policy decision and platform design. We must defend a web that is free and unfettered, and improve connections that allow creativity and collaboration. We should leave the artificial to the machines and restore humanity to the users.

4. Surveillance Capitalism after 'Singularity' and Prospects of Information Civilization

4.1 Surveillance and Big Data

Big Data intensifies certain surveillance trends associated with information technology and networks, and is thus implicated in fresh but fluid configurations. According to Lyon, this is considered in three main ways: One, the capacities of Big Data (including metadata) intensify surveillance by expanding interconnected datasets and analytical tools. Existing dynamics of influence, risk-management, and control increase their speed and scope through new techniques, especially predictive analytics. Two, while Big Data appears to be about size, qualitative change in surveillance practices is also perceptible, accenting consequences. Important trends persist – the control motif, faith in technology, public-private synergies, and user-involvement – but the future-orientation increasingly severs surveillance from history and memory and the quest for pattern-discovery is used to justify unprecedented access to data. Three, the ethical turn becomes more urgent as a mode of critique. Modernity's predilection for certain definitions of privacy betrays the subjects of surveillance who, so far from conforming to the abstract, disembodied image of both computing and legal practices, are engaged and embodied users-in-relation whose activities both fuel and foreclose surveillance (Lyon 2014: 1).

Big Data practices echo several key surveillance trends but in several respects they point to realities that have perhaps been underestimated, he analyzes. One is that, within surveillance studies there has been a general tendency to analyze multiple forms of surveillance that are not directly linked with state-based, top-down surveillance of the kind epitomized in George Orwell's Nineteen-Eighty-Four. If this was understood by some to mean that more generalized – or, following Gilles Deleuze, "rhizomic" – surveillance spells less state surveillance activity (Lyon 2014: 10-11; Clavel).

In a sense, he insists, this means that Orwell's bleak vision of what tendencies in post-war liberal democratic polities could lead to authoritarian surveillance regimes were not mistaken so much as standing in need of complementary analyses, such as that of his contemporary, Aldous Huxley, in Brave New World, Big Data practices in consumer surveillance are co-travelers with those of state surveillance and together produce the kinds of outcomes around which ethical debates should now revolve. Indeed, not only are they 'co-travelers,' they also cooperate extensively, the one taking methods from the other, with, as discussed above, potentially pernicious results as the 'successful' methods in one area are applied in ways deleterious of human rights in another (Lyon 2014: 11).

It is these matters in particular that attract critique, he insists, especially in relation to anticipatory and preemptive approaches common to Big Data mindsets and activities and amplifying what is a long-term surveillance trend. These fit neatly with currently intensifying political styles of neo-liberalism that, with regard to 'national security,' are seen in a list towards actuarialism and a consequentialist concern with managing disorder and crime rather than seeking its causes and attempting to eradicate them (Lyon 2014: 11; Lyon 2018; Big Brother Watch).

4.2 Surveillance, Facial Recognition, and Right to Obscurity

We have a right to maintain our anonymity such that our mundane activities, behaviors, and associations are not recorded and linked to our identity by means of facial recognition surveillance. Kaplan explains that the mere collection of this non-anonymous data makes us vulnerable to significant harms in the forms of psychological manipulation and opportunity loss. In addition, this right to obscurity is not outweighed by social interests in preventing crime and violence or locating missing persons. These social interests could be equally served while still preserving individuals' anonymity by dissociating location data from personal identities and by only analyzing behavioral patterns from anonymous data. Since the risks of psychological manipulation and opportunity loss could be greatly reduced by maintaining these protections to public anonymity, implementing facial recognition surveillance without protecting people's anonymity as obscurity in public would impose an unnecessary and, thus, unjust risk of harm (Kaplan: 18-19).

The right to anonymity as obscurity is here grounded in the broader societal interest within liberal democracies that individuals can effectively exercise their rights and liberties, he continues. The implicit intimidation of using facial recognition surveillance to catalog political and religious participants fails to communicate to individuals that they are not vulnerable to state's power to impose negative repercussions for their activities and convictions. Given the asymmetry of power between those under surveillance and the institutions carrying out the surveillance, the state has a special obligation to reassure individuals that they will not be subject to negative repercussions when they exercise their rights to free speech, assembly, and worship. Reassurance here can only take the form of banning the use of real-time facial recognition surveillance to catalog participants in political and religious activities. This second right to obscurity while in public is also not overridden by competing social interests. The only justifying purpose for such cataloging is for the sake of a criminal or legal investigation and, for such instances, the real-time use of facial recognition is not required. A warrant can be required to apply this technology post factum to whatever video recordings we have of a crime scene or the like (Kaplan: 19).

If we recognize these two rights to anonymity as obscurity in public, how radically will this alter how we conceive of privacy? He insists that this question proves difficult to answer given the conceptual disarray surrounding privacy. However, protection against collecting non-anonymous surveillance data that can so easily be aggregated and analyzed into detail psychological profiles maps very closely to two different popular conceptions of privacy: control over intimate information and protection of the integrity of the person. That the obscurity and privacies interests coincide so closely may indicate that anonymity is here a means of protecting privacy. On the other hand, it appears that the societal interest in protecting the anonymity of people publicly engaged in political and religious activities is not readily connected to privacy interests. The apparent independence of this obscurity right indicates that advocacy for protections against using real-time facial recognition to catalog participants is protests, rallies, and religious observances ought to be made without appealing to privacy so as to avoid muddying the waters (Kaplan: 19; Gates).

4.3 Surveillance Capitalism and Prospects of Information Civilization

Zuboff describes an emergent logic of accumulation in the networked sphere, ‘surveillance capitalism,’ and considers its implications for ‘information civilization.’ She sheds light on the implicit logic of surveillance capitalism and the global architecture of computer mediation upon which it depends. This architecture produces a distributed and largely uncontested new expression of power: ‘Big Other.’ It is constituted by unexpected and often illegible mechanisms of extraction, commodification, and control that effectively exile persons from their own behavior while producing new markets of behavioral prediction and modification (Zuboff 2015: 75).

Individuals quickly came to depend upon the new information and communication tools as necessary resources in the increasingly stressful, competitive, and stratified struggle for effective life, she continues. The new tools, networks, apps, platforms, and media thus became requirements for social participation. Finally, the rapid buildup of institutionalized facts – data brokerage, data analytics, data mining, professional specializations, unimaginable cash flows, powerful network effects, state collaboration, hyperscale material assets, and unprecedented concentrations of information power – produced an overwhelming sense of inevitability. These developments became the basis for a fully institutionalized new logic of accumulation that is called surveillance capitalism. In this new regime, a global architecture of computer mediation turns the electronic text of the bounded organization into an intelligent world-spanning organism: Big Other. New possibilities of subjugation are produced as this innovative institutional logic thrives on unexpected and illegible mechanisms of extraction and control that exile persons from their own behavior (Zuboff 2015: 85).

Under these conditions, she insists, the division of learning and its contests are civilizational in scope. To the question 'who participates?' the answer is – those with the material, knowledge, and financial resources to access Big Other. To the question 'who decides?' the answer is, access to Big Other is decided by new markets in the commodification of behavior: markets in behavioral control. These are composed of those who sell opportunities to influence behavior for profit and those who purchase such opportunities. Google's rendering of information civilization replaces the rule of law and the necessity of social trust as the basis for human communities with a new life-world of rewards and punishments, stimulus and response. Surveillance capitalism offers a new regime of comprehensive facts and compliance with facts. It is a coup from above – the installation of a new kind of sovereign power (Zuboff 2015: 85-86).

The automated ubiquitous architecture of Big Other, she insists, its derivation in surveillance assets, and its function as pervasive surveillance, highlights other surprising new features of this logic of accumulation. It undermines the historical relationship between markets and democracies, as it structures the firm as formally indifferent to and radically distant from its populations. Surveillance capitalism is immune to the traditional reciprocities in which populations and capitalists needed one another for employment and consumption. In this new model, populations are targets of data extraction. This radical disembedding from the social is another aspect of surveillance capitalism's antidemocratic character. Under surveillance capitalism, democracy no longer functions as a means to prosperity; democracy threatens surveillance revenues (Zuboff 2015: 86).

Will surveillance capitalism be the hegemonic logic of accumulation in our time, or will it be an evolutionary dead-end that cedes to other emerging information-based market forms? What alternative trajectories to the future might be associated with these competing forms? She concludes that the prospects of information civilization rest on the answers to these questions (Zuboff 2015: 86; Zuboff 2019a; Zuboff 2019b; Zuboff 2021).

In short, the big companies are both rewriting the rule of capitalism and rewiring the circuit of power. The Googles, Facebooks, Alibabas and Tencents of our world are ushering in a new form of capitalism by monetizing data-derived behavioral insights at an unprecedented scale and effectiveness. More alarmingly, the surveillance capitalism threatens to metastasize into a scary new form of power 'instrumentarianism'. We should switch to those privacy-by-design services of which we approve and delete those apps that rely on excessive surveillance. The inexorable extension of surveillance technologies, which are so widely used to counter terrorism and serious crime, will overwhelm any hopes we may have of remaining anonymous. Our future is already being built in China where facial recognition technology is ubiquitous and uncontestable. But it is dangerous to pursue purely technological solutions to human challenges because technology cannot solve anything by itself. In May 2019, San Francisco became the first city in the US to ban the official use of facial recognition technology. We should all be concerned about how such technology is used to police society and we still have the power to shape the legal framework in which it operates.

5. Conclusions

Although films such as 'Minority Report' and 'Robocop' may not present the most attractive depiction of the future of advanced technologies in law enforcement, understanding how these technologies can be applied by law enforcement agencies for the safety and security of our global community is of critical importance.

AI and robotics are new concepts for law enforcement, and many national law enforcement agencies are already actively exploring the application of AI and robotics to enhance crime prevention and control. The level of engagement of national law enforcement agencies in AI and robotics is far from homogenous, with some countries being more advanced than others in their exploration of these technologies. Some countries with particularly mature experience, have even established an official function within their organizations to envision AI and robotics use cases for law enforcement. Common features across the board however, are modesty with respect to national capacities and an eagerness to develop experience.

Although there is a broad spectrum of potential law enforcement use cases, a common transversal theme associated with many of these use cases is enhanced surveillance capabilities. Of course, with any type of surveillance, the potential impact on the fundamental human right to privacy as recognized by the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR), as well as the numerous other international and regional legal instruments, is an essential consideration. Indeed, as the use of AI and robotics by law enforcement becomes more pervasive throughout society, touching ever more upon the lives of citizens, it becomes increasingly important for law enforcement to ensure that the use of these technologies is ethical.

Law enforcement is an important test case with respect to privacy and ethics in the use of AI and robotics, predominantly because privacy is generally more likely to be trumped by security in the law enforcement community. If law enforcement can take the leadership, set norms and establish councils or bodies for the ethical use of AI and robotics, other communities may follow. Law enforcement also has the unique advantage to be discussing these issues before the use of AI and robotics becomes a common feature in law enforcement. If this opportunity is ignored and AI and robotics are used in law enforcement without 'fairness, accountability, transparency and explainability' then the law enforcement community risks losing the confidence of the communities and citizens that it is mandated to protect.

Democratic principles should be built into our technologies. This include human rights and human dignity, freedom and self-determination, pluralism and protection of minorities, the division of power, checks and balances, participatory opportunities, transparency, fairness, justice, legitimacy, anonymous and equal votes, as well as privacy in the sense of protection from misuse and exposure, and a right to be let alone. In the future, the principle to be legally and technologically established would be that we decide who is allowed to use what data for what purpose, period of time and price. Uses of personal data, also statistics created for science and for politics, would have to be transparently reported to individuals. We would have to upgrade our system toward a 'multidimensional real-time feedback system'. Such a multidimensional incentive and coordination system is needed manage complex systems more successfully and also to enable 'self-organizing, self-regulating systems'.

[References]

Aguirre, K., Badran, E., and Muggah, R. (2019). *Future Crime: Assessing twenty first century crime prediction*. Rio de Janeiro: Igarape Institute.

Big Brother Watch (2018). *The State of Surveillance in 2018*.

Bostrom, N. (2014). *Superintelligence: Paths, Dangers, Strategies*. Oxford: Oxford University Press.

Brundage, M., Avin, S., Clark, J., Tonor, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B., Anderson, H., Roff, H., Allen, G. C., Steinhardt, G., Flynn, C., Éigeartwigh, S. Ó., Beard, S., Belfield, H., Farquhar, S., Lyle, C., Crootof, R., Wvans, O., Page, M., Bryson, J., Yampolskiy, R., and Amodei, D. (-). *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*. Future of Humanity Institute, University of Oxford, Centre for the Study of Existential Risk, University of Cambridge, Center for a New American Security, Electronic Frontier Foundation, and OpenAI.

Clavel, G. (-). *La Gouvernance de l'Insécurité : La pénaisation du social dans une societé sécuritaire*. Paris : L'Harmattan.

Collegium Helveticum (2018). *Automated Justice: Algorithm, Big Data and Criminal Justice Systems*. EURIAS-Conference. Zürich: Universität Zürich.

Ferguson, A. G. (2017). *The Rise of Big Data Policing: Surveillance, Race and the Future of Law Enforcement*. New York: New York University Press.

Gates, K. A. (2011). *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance*. New York and London: New York University Press.

Harari, Y. N. (2017). *Homo Deus: A Brief History of Tomorrow*. London: Vintage.

Hawking, S. (2018). *Brief Answers to the Big Questions*. London: John Murray.

INTERPOL and UNICRI (2018). *Artificial Intelligence and Robotics for Law Enforcement.*

Kaplan, S. (2018). *To Be a Face in the Crowd: Surveillance, facial Recognition, and a Right to Obscurity*. ECPR Conference 2018.

Konikoff, D., and Owusu-Bempah, A. (-). *Big-Data and Criminal Justice – What Canadians Should Know*. Broadbent Institut.

Kurzweil, R. (2005). *The Singularity Is Near: When Humans Transcend Biology*. London: Duckworth.

Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data and Society*: 1-13.

Lyon, D. (2018). *The Culture of Surveillance*. Cambridge: Polity.

Mainzer, K. (2016). *Künstliche Inteligenz – Wann übernehmen die Maschine?* Berlin: Springer.

McCarthy, O. J. (2019). *AI and Global Governance: Turning the Tide on Crime with Predictive Policing*.

O'Neil, C. (2016). *Weapons of Math Destruction: How Big Data increases Inequality and Threatens Democracy*. Penguin Books.

Selbst, A. D. (2017). Disparate Impact in Big Data Policing. *Georgia Law Review* 52: 109-195.

Simmons, R. (2016). Qualifying Criminal Procedure: How to Unlock the Potential of Big Data in our Criminal Justice System. *Michigan State Law Review* 2016: 947-1017.

Takemura, N. (2020). From 'Rule of Law' to 'Algorithmic Governance': Three Minimum Basic Principles for Prediction and Automation in Criminal Justice System —

'Fairness', 'Accountability', and 'Transparency' — (In Japanese). *Toin Law Review* 27 (1): 43-72.

The Law Society Commission on the Use of Algorithms in the Justice System and The Law Society of England and Wales (2019). *Algorithms in the Criminal Justice System.*

Tréguer, F. (2019). La《ville sûre》ou la gouvernance par les algorithmes. *Le Monde diplomatique*, juin 2019 : 22-23.

Van der Sloot, B., Broeders, D., and Schrijvers, E. (eds.) (2016) *Exploring the Boundaries of Big Data.* The Hague/Amsterdam: Amsterdam University Press.

Završnik, A. (2018). Big data: What is it and why does it matter for crime and social control? In: A. Završnik (ed.) *Big Data, Crime and Social Control.* London and New York: Routledge. 3-28.

Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology* 30: 75-89.

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

Zuboff, S. (2019b). Un capitalisme de surveillance. *Le Monde diplomatique*, Janvier 2019 : 1, 10-11.

Zuboff, S. (2021). The coup we are not talking about. *The New York Times International* February 3: 12, 14.