The Political Economy of Communication
7(2), 3–27

http://www.polecom.org

The Algorithm made me do it! Technological transformations of the criminal justice system

Oscar H Gandy Jr., Annenberg School for Communication, University of Pennsylvania

Keywords: Artificial intelligence, criminal justice system, inequality, race, surveillance technology

Abstract

Communication and information scholars have joined others in expressing concern about the impact of algorithmic techniques on the generation of strategic intelligence for corporate and government decision-makers. Their attention to the impact of these systems on policing and the criminal justice system has developed somewhat more recently. This article examines those concerns as they apply to the use of algorithmic systems by urban police, judges, and other central actors within the criminal justice system in the United States, with references to related developments around the globe. Although the use of cameras for the surveillance of target areas within urban centers has been the subject of critical assessment almost from the beginning of their use, much of that work was focused on the behavior of the human monitors that determined what the central focus of those cameras would be, as well as the nature of the behaviors that would trigger the movement of officers to the scene. Increasingly, however, the work of human monitors has been re-assigned to semi-autonomous computer systems, guided by artificial intelligence resources, and updated routinely through the use of machine learning techniques. The development of these enhanced systems involves a number of related functions that are transforming the nature of policing. My critical examination of this development focuses on the following elements: 1) the capture and use of images from mobile cameras, 2) the analysis of social networks, and 3) the evaluative assessment of members belonging to algorithmically classified groups. This article will explore these developments with special regard to their likely impact upon the life chances and well-being of members of racialized population segments. It concludes with suggestions for addressing societal threats to the rule of law as they apply to policing within the Criminal Justice System.

Christian Sandvig and his colleagues (Sandvig et al., 2016) helped to set the research agenda for communication and information scholars concerned about how algorithmic techniques were generating strategic intelligence for corporate and government decision-makers. Much of the research that followed was focused on the nature and extent of the biases and errors that emerged

when assessments and recommendations affected the life chances of racial and ethnic minority population segments (Barocas and Selbst, 2016). This article examines those concerns as they apply to the use of algorithmic systems by urban police, judges, and other central actors within the criminal justice system (CJS) in the United States (US). However, as Shoshana Zuboff (2019) makes clear, even though this is a technology that might be identified as an American invention, the use of artificial intelligence for surveillance purposes has become a global reality that no nation can ignore.

Mireille Hildebrandt (2018) identifies her efforts, in a recent article, as seeking to promote the concept and practice of "legal protection by design" with the purpose of bringing "artificial legal intelligence under the Rule of Law" (3). Hers is an important mission, one that can be distinguished from the efforts of engineers and researchers whose goals are focused on improving the accuracy and reliability, and perhaps even the fairness of the predictions, recommendations, and increasingly the decisions being made by artificially intelligent machines. Hildebrandt (2018) identifies four attributes of reliance on artificial legal intelligence that she suggests may "disrupt the concept and the Rule of Law". Firstly, the inaccessibility of the software used in rendering decisions may make them "inscrutable and thereby incontestable". Secondly, "the shift from meaningful information to computation entails a shift from reason to statistics, and from argumentation to simulation". Thirdly; "a set of fundamental rights may be infringed, compromised or even violated". Fourthly, "to the extent that the algorithms become highly proficient… lawyers may outsource part of their work". Consequently, they become deskilled and lose their ability "to check whether the software 'gets it right', confronting us with a new Catch 22" (11-12).

Whereas Hildebrandt's attention is focused on deskilling among lawyers, and perhaps even judges, this article will focus primarily on the consequences that flow from the deskilling of the police officers who play such a critical role within the CJS. Following an examination of the variety of transformative changes taking place within the CJS, we examine the form and function of the algorithmic systems that are largely responsible for transformations in the nature of policing. Focusing primarily on cameras and associated audiovisual technologies with fixed and mobile applications, this initial review will consider the usage of these systems in providing biometric identification and evaluative assessments. An important part of the technology that enables this work, beginning with identification, is mathematical or computational. A large part of the computation that identifies us as individuals, as well as members of variously defined groups, uses massive amounts of transaction-generated-information (TGI). It is important to note that only a miniscule fraction of this information has actually been generated by the individuals who become the focus of attention by the police. Much of it has been derived from a process of statistical analysis of independently gathered data. This process of remote sensing through the analysis of data (Gandy, 2012), is becoming more powerful with developments in artificial intelligence.

Following a technological review, we shift our attention to the surveillance economy, a rapidly evolving marketplace dominated by a comparatively small number of firms. The relationships between these market leaders and the actors and entities that make up the CJS invite consideration of the police, the prosecutors, and the judges, but also the people who are the targets of surveillance. They struggle to gain access to the data that determines the quality of life that they, their families, and their communities will get to enjoy.

The criminal justice system

The criminal justice system (CJS) is a complex amalgam of bureaucratic and administrative agencies that lend support and guidance to specialized agents responsible for the exercise of informed judgment about the use of force in their efforts to reduce crime and protect the public from those who would engage in criminal behavior. The CJS also contains a multidimensional network of judicial personnel, including those working at different levels across a system of courts, and yet another network of specialists that manage the penal system. In the United States, these agencies operate within jurisdictions that range from cities through counties, states and the nation as a whole. At some level, every unit of this complex system relies upon information technology to capture, store, process and share information about the individuals, groups, and entities that somehow attract its attention. The nature of their relations to these objects of interest is continually being transformed by changes in the systems they have come to rely on.

It is important to understand the stages and character of the interactions that individuals have with decision-makers at different levels of the CJS. In one sense, there is value in thinking about these interactions in terms of a path or a route along which individuals might pass throughout their lives, from birth to death. The nature of these interactions with the CJS varies widely, although race, ethnicity, gender, social class, and place of residence are among the factors that have emerged as important determinants of the relevant outcomes.

Let us assume that the earliest interactions between an individual and a member of the CJS involves little more than observation. Depending on the observer and the behavior being observed, the next interaction might involve a friendly greeting, or a request to stop, respond to questions, and consent to a search. It is of course possible that the end of an interaction beginning with observation might end with an arrest. Further interactions influenced by the nature of the prior interactions with the CJS, may involve interactions with prosecuting and defense attorneys, and eventually with a judge. This particular string of interactions may end with a conviction and a sentence, or in some cases, with an execution. At every step along the way, an agent of the CJS will have made critical assessments and decisions about what happens next based on personal beliefs, professional standards, and understandings of how the law applies to the behavior observed, or assumed, on the basis of other information being brought to bear.

The bases upon which these decisions have traditionally been made within the CJS are being altered fundamentally by the nature of the information being added to that which had previously been available to a decision-maker. The fact that this information is the product of analytic procedures, increasingly carried out by autonomous, or semi-autonomous machines is changing the nature of the process, the characteristics of its outcomes, and its impact on the quality of life enjoyed by members of different populations segments around the globe.

The development and use of analytical resources to enhance and improve the kinds of decisions arrived at within the CJS often have a cyclical pattern, perhaps associated with the emergence of a particular kind of crime wave, such as those associated with the distribution of drugs. The current expansion in the development and adoption of predictive technologies has been associated with the 2008 recession, which limited the ability of local and regional governments to manage the demands for public services, including those of the CJS (Brayne, 2017; Ferguson, 2017).

Increased reliance upon classificatory, evaluative and predictive technologies within the CJS has not gone without criticism, much of which has been focused on the nature of the bias and error that remains in the systems being developed, promoted and used. The use of decision assistance

technology by judges and prosecutors is criticized on the basis that they may amplify and naturalize longstanding racial biases, all the while making them more difficult to recognize, understand and correct (Browne, 2015; Burrell, 2016; Campolo et al., 2017).

Sophisticated decision-assistance systems such as those which recommend sentences, bail, probation and drug testing are not designed to replace human managers within the CJS. Their purpose is to assist them in choosing the appropriate opportunities or constraints that will benefit a particular individual in relation to a particular set of circumstances (Cino, 2018). However, the fact is that these systems have not actually been designed for application to a particular individual. Instead, they have been designed for members of a population segment that share a similar pattern of lifetime experiences. This source of unmeasured variance across a variety of contexts heightens the challenges involved in evaluating the performance of these systems (Bollier, 2018).

Transformations of policing

There has been a fundamental shift toward a "more proactive, predictive and... pre-emptive policing" that is marked by "increased reliance on surveillance technology" (Van Brakel and De Hert, 2011-13: 165). This approach differs from the "standard model of policing, which involves an emphasis on reacting to particular crime events after they have occurred, mobilizing resources based on requests coming from outside the police organization, and focusing on the particulars of a given criminal incident" (Weisburd and Majmundar, 2017: S-1).

However, an increasingly important use of this technology involves a form of profiling, generally understood as the assignment of individuals to "groups" on the basis of shared attributes, including behaviors predicted on the basis of correlations generated algorithmically through the processing of data not necessarily associated with criminal activity (Linder, 2019). Among several approaches to proactive policing, one identified as a "place-based approach" incorporates a number of technologically based strategies and resources that are based on evidence "for the concentration of crime at micro-geographic places" (Weisburd and Majimundar, 2017: 2-4). Those places then become targets for predictive or 'hot spots policing' and the strategic placement and monitoring of closed-circuit television cameras (CCTV).

These strategies differ from person-focused strategies, including those which concentrate attention on repeat offenders, and those which rely upon "stop, question, and frisk" interactions with pedestrians. Both of these differ markedly from "community-based" approaches that seek to develop collaboration between police and members of a particular community (Weisburd and Majimundar, 2017: S-2). Whereas place-based and person-focused approaches are often evaluated in terms of the impact those strategies have on the community's attitude toward the police, community-based strategies "specifically seek to reduce fear, increase trust and willingness to intervene in community problems, and increase trust and confidence in the police" (Weisburd and Majimundar, 2017: S-6–S-7). The somewhat limited number of reported studies suggest that "community-oriented policing contributes modest improvements to the community's view of policing and the police in the short term."

Although predictive policing has been said to be the "holy grail of policing—stopping crime before it happens" (Ferguson, 2017: 1117), evidence clearly suggests that we are at the early stages of its development. The uses of this technology within police departments so far have been focused in a fairly limited number of predictive applications. These are: predicting the places and times in which particular types of crimes are more likely to occur; predicting and identifying those individuals who are most likely to commit those crimes; and identifying individuals who are most

likely to become the victims of crime (Degeling and Berendt, 2018). Other applications by police departments include social network analysis, involving social media content which generates a variety of maps that "link friends, gangs, and enemies in a visual web of potential criminal actors" who might be approached in time to prevent some of the violent interactions that are common to these networks (Ferguson, 2017: 1118, 1145). Arguably, these applications of predictive algorithms go beyond mere prediction to a level of understanding about the "hidden crime-inducing environmental conditions which can be deterred by an intentional police response" (Ferguson, 2017: 1121).

What they all have in common is an increased reliance upon data gathering and analysis. This substitution of data for intuition alters the traditional relationships between individual officers and their background, experience and knowledge of the forces that shape the rise and fall of crime over time (Moses and Chan, 2018). This shift may also weaken the constitutional protections that previously limited the ability of police to use strategies that might "raise concerns about deeper legal values such as privacy, equality, autonomy, accountability, and transparency" (Weisburd and Majimundar, 2017: S-4). On the other hand, these transformations in policing associated with big data analytics may actually help to focus attention on the behavior of police in ways that might identify patterns of unconstitutional acts. An important part of such a development might be a shift from the traditional focus on the "one bad apple" within a department, toward a search for patterns of behavior indicative of "systemic racial bias" (Ferguson, 2019: 561).

These changes in the nature of policing associated with greater reliance upon technologies that provide evaluative assessments of individuals who come into the view of police with cameras invites consideration of the kinds of decisions that officers have to make before moving from observation to interactive intervention. Some of those decisions are based upon statutes or court decisions. The extent to which camera-based systems will make recommendations on the basis of algorithmic assessments of probable cause or reasonable suspicion is something yet to be decided. It seems likely, however, that judgments made by officers in the future will be influenced by what the device recommends, with or without an accompanying rationale. For example, what was initially a fairly meaningful standard has been, over time, relaxed for particular kinds of searches so that officers only needed to have a "reasonable suspicion" that an individual was criminally active (Miller, 2014). Once again, consideration of the nature and extent of false positives that are likely to be generated by the automated surveillance of millions of innocent persons will require a formal determination by the courts or the legislatures. Are the burdens being imposed on the public justified by the accumulated benefits of reductions in different kinds of crime?

A number of factors related to the nature of predictive policing actually make it difficult to provide reliable estimates concerning the impacts of its use (Moses and Chan, 2018: 810-813). This is because the "practice of predictive policing itself affects the data collected," essentially by affecting what is being measured. As a result, "predictive accuracy cannot be measured simultaneously with programme effectiveness" (Moses and Chan, 2018: 810-813) A related concern raised by Moses and Chan is that predictive policing tends to be spatially focused. In their view, "an approach that focuses on place... risks also focusing on only particular categories of crime." And such a focus is likely to increase the accumulation of the negative burdens that often accompany this kind of focus on poor and minority communities.

This perspective is echoed by Stefan Kaufmann (2016) who argues that "the problem widely faced by technology is that of dealing with reliability at the technological standards level in terms of the tension between *false positives* and *false negatives*" (83). As he concludes in his review of the

problems involved when making evaluative determinations of security technology, it is difficult to analyse the "constellations of power" involved in the "conceptual translation of social norms into technical norms." He suggests that we need to understand that the costs involved in producing too many false positives or false negatives have to be understood in relation to "whose security is enhanced through specific technologies.... and who in consequence might become more vulnerable" (Kaufmann, 2016: 93).

A major source of concern for police is the likely consequences of greater reliance upon information and strategic recommendations derived from algorithmic assessments. Of particular importance is the belief that individual officers will become increasingly unable to provide their own reasons for deciding to stop and search a particular pedestrian at a particular time and place. Mark Andrejevic (2019) notes that the strategies arising from automated algorithmic processing of the massive amounts of data captured through "always-on sensing networks" are enabling "prediction and pre-emption to replace deterrence" (7). Automated surveillance systems benefit from a "continual process of experimentation and environmental modulation", which enables the anticipation and foreclosure of devalued behavioral options through targeted interventions (10). As a result, the panoptic infrastructure described by Foucault arguably becomes superfluous once "discipline is internalized" algorithmically.

In an earlier assessment of the socio-technical systems that mark the emergence of "surveillance capitalism," Zuboff (2015) offers a similar framing of the production of "radically distributed opportunities for observation, interpretation, communication, influence, prediction, and ultimately modification of the totality of action" (82). Like Andrejevic, Zuboff (2019) focuses on the use of these systems to "shape our behavior at scale," which means that "it is no longer enough to automate information *flows about us*; the goal is now to *automate us*" (8).

As the police rely more on algorithmically-derived guidance about whom to stop, question and search, the constitutional requirements for an officer to have an individual basis for suspicion seem likely to be erased completely, rather than merely ignored by the courts (Blount, 2017; Ferguson, 2012, 2015; Joh, 2016; Goel et al., 2017; Mateescu et al., 2015; Miller, 2014). This "automation bias effectively turns a computer program's suggested answer into a trusted final decision" (Citron, 2008: 1272). As a result, before very long, saying that "the algorithm made me do it" will no longer be required, it will simply be assumed, because the development of reasonable suspicion has been outsourced to a computer (Berman, 2018: 1325; Joh, 2017: 125).

Increased reliance on algorithmic systems with regard to interactions with individuals overlaps with concerns about the maintenance of evidence related to cases under court jurisdiction. Concerns about police management of evidence emerge primarily from two directions: one associated with limited resources, knowledge and capabilities; and the other associated with self-interest, whereby law enforcement personnel may attempt to modify records to achieve goals or avoid critical sanctions. Furthermore, there are even more concerns being raised about "having some or all digital evidence stored, maintained, and accessed through a private third party that is an economic stakeholder whose customer is police departments" (Wood, 2017: 42).

Wood notes that "[t]hese issues become further complicated when the footage is processed, stored, described, and retrieved using cloud-based evidence-management systems such as Evidence.com" (Wood, 2017: 45) from Axon or one of their remaining competitors. Some of those complications have to do with the determination of data ownership rights, as Axon is arguably a co-creator of the data, and their dominant status in this rapidly developing field gives them an edge in negotiating the contracts governing usage of such data. Negotiated determinations concerning the

status of law-enforcement camera data as public records continue to challenge courts, states and municipal governments. This is the case, despite the common suggestion that widespread investment in cameras and data management services was designed to support both the transparency and the accountability of police with regard to their interactions with the public at large (Wenner, 2016).

Transparency and accountability

Transparency and accountability refer to the ability of the public, perhaps through their elected representatives, to evaluate and influence the manner in which these technologies are used to provide societal benefits. This, in turn, depends upon the ability of the public and their representatives to gain access to the information they need in order to produce meaningful assessments of system performance, economic efficiency, and the equitable distribution of costs and benefits throughout the population (Ananny and Crawford, 2016; Mateescu et al., 2016; Squillacote and Feldman, 2018). Many government agencies have organized, financed and collaborated with university-based researchers to evaluate the impact of body-worn cameras (BWCs) on the behavior of police officers and individuals who have interacted with police during criminal investigations. These investigations have led to mixed conclusions about their influence on both attitudes and behavior toward police and the technology (Ariel et al., 2015; Smykla et al., 2016; Yokum et al., 2017). There have been studies, however, which suggest that the behavior of police wearing such cameras has actually improved, at least with regard to measures that represent procedural justice (McCluskey et al., 2019).

Unfortunately, in regard to information about the use of technology by the police, a variety of barriers make it difficult to access the relevant information which is necessary for evaluation (Rieke et al., 2018). These include contractual agreements between public agencies and the private commercial firms that provide the devices and the data management services. They may involve the storage and processing of the transaction-generated information (TGI). Such agreements often limit the disclosure of details about the underlying operational systems, their development, testing, and performance (Joh, 2016). Those limitations become especially problematic when the assignment of resources and the implementation of crime prevention strategies are managed largely, if not completely, by autonomous systems (Rieke et al., 2018). This is part of the challenge we face in trying to separate the value of transparency from the exercise of power by those who seek to avoid any limitations on their use of these technologies (Ananny and Crawford, 2016). As Cohen (2017b) sees it, "the opacity that surrounds pervasive, networked surveillance raises the prospect of secret, unaccountable exercises of power—of government not by laws but rather by powerful corporate entities" (12).

An important insight in regard to the concerns associated with the increased role of automated technologies is that governmental agencies, especially those responsible for the management of the criminal justice system (CJS), are constrained by their budgets. As a result, many of these agencies rely upon commercial vendors of surveillance systems that have sought and received legislative, judicial or contractual protection against requests to share information about how assessments, recommendations and decisions are being made. As many see it, when "a government agent implements an algorithmic recommendation that she does not understand and cannot explain, the government has lost democratic accountability" (Brauneis and Goodman, 2018: 109). Part of the accountability problem has to do with the determination of who (or what) is accountable to whom. Algorithmic accountability involves the assignment of responsibility to the data scientists, software

and applications engineers that design the systems (Binns, 2018; Caplan, et al., 2018). It also includes the managers of corporate and governmental agencies who negotiate the contracts that specify the kinds of assessments and recommendations that they expect their devices or services to provide (Goldenfein, 2018). It seems likely, however, that system operators "will offer explanations that appeal to standards which they themselves endorse; but which may not be accepted by those whom the decision affects" (Binns, 2018: 548).

The widespread adoption of body-worn cameras (BWCs) by police departments was viewed by many advocates as an opportunity for the public, especially those in racialized communities who were often the victims of aggressive policing, to benefit from increases in transparency and accountability regarding police behavior (Beutin, 2017). Unfortunately, the audio and video evidence captured by these cameras are generally placed under the control of the police departments, or held within a contractually mandated joint operational arrangement with the vendor of the cameras and the management of evidentiary materials (Sacharoff and Lustbader, 2017; Yu et al., 2017). President Obama's Task Force on 21st Century Policing is said to have acknowledged the growth of video footage from personal cameras in the telephones used by members of the public that are distributed widely through social media. In these circumstances, the police need to ensure that video from an officer's perspective can also be made available for the public to view (Obama, 2017). However, from a critical perspective (Beutin, 2017) "the report makes it clear that its main endorsements of and reservations with cameras lie in protecting the police" (15). Although the initial public support for the acquisition and use of the cameras emphasized their capacity to improve the transparency and accountability of police officer behaviour, the evidence to date suggests that these resources are primarily used to prosecute "ordinary criminal cases, including misdemeanors such as resisting arrest and more serious drug offenses." Data and critical analyses also suggest that "body camera videos are used far more often against ordinary citizens than the police" (Sacharoff and Lustbader, 2017: 273-4), although a number of studies have reported reductions in the use of force by police following the adoption of BWCs (Chen, 2017; White and Fradella, 2018). The use of BWCs is associated with poor program implementation resulting in consequences ranging from "resistance among line officers to low usage by downstream criminal justice actors and backlash from citizens" (White and Fradella, 2018: 1586). An extensive review of 129 policies from police agencies that had been funded by the US Department of Justice (DOJ) led to the conclusion that "implementation of a BWC program comes with a high degree of difficulty, and the consequences of implementation failure are significant" (White and Fradella, 2018: 1636-1637). In part, this is because "combatting police misconduct is complex and goes far beyond quick fixes (e.g., increased training) or removing a few 'rotten apples' that consistently make poor decisions."

After this brief introduction to the CJS, with its special focus on the impacts that result from the routine activities of police officers, we turn our attention to the nature of the technological systems and the multiple functions and goals they are thought to serve within the CJS.

Surveillance and its functions

Surveillance is generally understood as referring to the gathering of information about people, places and things. The functions of surveillance involve several different, but related operations beginning with identification, proceeding to classification, evaluation, prediction and, in a great many cases, attempts to influence the behavior of a relevant other. Within the criminal justice

system (CJS), the relevant others are nearly always human beings. Over time, we have come to think about identification as part of a tightly linked process which associates an individual's identity with tokens of identification that include their names and documents, including birth certificates, drivers' licenses and passports. The primary relationship between these initial sets of markers is the assumption, and perhaps the legal determination that they all relate to a unique individual. Elements of this initial set may also be tightly linked with other attributes of identification that may be shared with a good many other individuals, such as age, race, gender, height and weight.

Distinctions are often drawn here between identity and identification. An individual's identity is primarily the result of personal reflection and assessment, something closely associated with individual autonomy, although the influence of others on that determination cannot be denied. Identification, on the other hand, is almost entirely influenced and determined by others, although the individual so identified may have participated in that process by answering a question or checking a box. Thus, many of the terms used in identification at this level may be the result of a classificatory exercise that differs in terms of procedure and terminology between different segments of the CJS (Gandy, 2009).

Margaret Hu (2017: 639) introduces us to what she calls "Algorithmic Jim Crow" as a socio-technical development that "exploits cybersurveillance and dataveillance systems that are rapidly proliferating in both the public and private sectors". Hu emphasizes the historical continuity of racial and ethnic classification, beginning with the creation of legal and regulatory constraints on the freedom of African Americans that were enforced even after the passage of the Thirteenth, Fourteenth and Fifteenth Amendments. She suggests that the classification of identity "is an essential step in establishing exclusionary systems" (Hu, 2017: 654). However, she notes that an additional step, which she refers to as, "screening," incorporates additional forms of documentation or evidence to determine the extent to which the individual has been following the rules established for the behavior of persons assigned to an excluded category (Hu, 2017: 655-656).

While Eubanks' (2018) critical engagement with the impact of algorithmic assessments includes African Americans, her primary focus is on inequality and the variety of ways in which automated systems punish the poor. For Eubanks (2018), policing "is broader than law enforcement: it includes all the processes by which we maintain order, regulate lives, and press people into boxes so they will fit our unjust society" (215). Consistent with the views expressed by Andrejevic (2019), Eubanks (2018) suggests that "the digital poorhouse makes the physical institution of the prison less necessary" (215).

David Lyon (2003) refers to this screening process as a form of "social sorting," that generates classifications that "are designed to influence and to manage populations and persons thus directly and indirectly affecting the choices and chances of data subjects" (13). He emphasizes the use of searchable databases as part of an emergent trend "towards attempted prediction and pre-emption of behaviors, and of a shift to what is called 'actuarial justice' in which communication of knowledge about probabilities plays a greatly increased role in assessments of risk" (Lyon, 2003: 15-16).

The classification of individuals may reflect the nature of the interactions that they have previously, or currently have with some unit of the CJS, such that they can be referred to as a suspect, victim, arrestee, juror, convict, prisoner, or parolee. Members of the CJS, especially those involved in law enforcement, are likely to employ a host of other classifications that identify an individual in terms of their past behavior or associations likely to have predictive value. Beyond classification, identification takes on a critically different meaning and importance when its focus turns to predictions about how likely an individual, or a member of a categorized group, will

respond in a particular way to an opportunity or a challenge. An additional feature of this process often involves an evaluative assessment or an estimation of the positive or negative values that would be derived from, or associated with, a particular set of behavioral responses. Increasingly actuarial assessments of these outcomes are compared in terms of risks to be minimized or avoided. What is currently treated as the final stage in this process of identification are recommendations that should be followed in order to increase the probability that the target, or target group members will respond in a desirable way. The efforts of police and other members of the CJS to improve their level of success in the identification, classification, evaluation and behavioral management of subject populations is increasingly dependent upon their use of sophisticated surveillance technologies.

The rate of change in the capabilities of surveillance technology makes it difficult to develop the legal, judicial and regulatory policies needed to ensure that the public interest and social values associated with democratic governance continue to be available. In the age of big data analytics, the success of corporations is tied to their ability to convince public and private actors that they need to identify, characterize and evaluate the individuals with whom they will interact. We can expect that decision-makers within the CJS will come to rely even more on products and services that provide these forms of identification almost as soon as they are developed enough to be demonstrated, or at least described, in promotional material (Joh, 2017).

Surveillance technology: Cameras, fixed and mobile

Although we are focusing our attention primarily on the use of cameras by law enforcement agencies, visual imagery has been used for centuries as a means of identification and classification of individuals and the groups to which they have been assigned (by authorities claiming the support of scientific theory and methods). Jake Goldenfein (2018) refers to Sir Francis Galton, the founder of British Eugenics, who used early photographs "to create 'composite' images intended to expose the 'mean' appearance of criminality" as an example of experimental strategies that actually failed to perform 6-7). Galton's efforts reflect a tendency to associate biological features with behavioral tendencies. As a result, he pursued the possibility of biometric assessments indirectly, despite the fact that both "phrenology and physiognomy had already been scientifically discredited by the time of Galton's experiments in 1877" (Goldenfein, 2018: 6-7). Despite those early failures, the same kinds of claims are being made for experimental work being performed today "using new photographic techniques, statistical methodologies, and biological theories" (Goldenfein, 2018: 14).

An extensive literature has been developed that explores the use of closed-circuit cameras (CCTV) by public and private organizations for the purpose of limiting losses associated with criminal activity in particular places (Ratcliffe et al., 2009). When combined with facial recognition technology (FRT), automated CCTV systems are likely to attract law enforcement, or other official responses to the presence of individuals whose images are already in miscreant databases. They usually contain an over-representation of the poor and minority members of the nearby community (Slobogin, 2002). Police departments in the US were encouraged to acquire and use body-worn cameras (BWCs) in response to public protests against police shootings, and as a resource that would protect police against false claims of abusing their power. As police agencies around the world adopted this technology, concerns arose about their impact on the police officers who wear them, as well as on members of communities most likely to be archived within digitized, evidence-managed systems (Chen, 2017; Palmer, 2016).

The use of the cameras and the records they generate tends to be under the control of the officers themselves as well as the agencies establishing and implementing policies about access and use of the data. This raises questions about access to, and use of those data by persons who have been recorded, as well as by other members of the CJS (Beutin, 2017; Mateescu et al., 2015). Additional concerns are expected to emerge as body-worn cameras (BWCs) capture and distribute continuous live-streamed audiovisual information to a central dispatch, either automatically, or upon a police officer's decision (Blount, 2017; Garvie and Moy, 2019; Hung et al., 2016). An early assessment of live facial recognition technology being tested by London's Metropolitan Police Service described how camera images were to be "streamed in real time to a facial recognition system". Comparisons would be made to determine if there was a "match" between the digital signature generated from the field, and those recorded in a "watchlist" database. In the event of a match, an alert would be made available to the officers in the field, and "a decision to intervene with an individual" might be made (Fussey and Murray, 2019: 19).

The use of facial recognition by law enforcement agencies highlights the absence of reasonable suspicion as multiple databases of photographic images are searched in pursuit of a match with images of a suspect or a person of interest. These databases are not limited to those of criminals, or even suspects. In most US states, merely having a driver's license puts thousands of innocents at risk of misidentification (followed by a stressful, if not actually dangerous interaction with a police officer) (Bedoya, 2017). That facial recognition systems presently in use have substantial error rates becomes especially troubling when we consider the fact that erroneous identifications are more likely to be made in searches for African Americans and members of other non-white racial or ethnic groups (Bedoya, 2017: 12-13).

Facial recognition technology is just one aspect of the biometric systems being developed to identify individuals (Goldenfein, 2018; Maurer, 2017). A recent US Government Accountability Office (GAO) report cited comments by the Electronic Frontier Foundation (EFF) about the error rates of these identification systems; "false positives can alter the traditional presumption of innocence in criminal cases by placing more of a burden on the defendant to show he is not who the system identifies him to be" (Maurer, 2017: 14). The GAO is concerned, in part, about the fact that the FBI has not made the investments necessary to ensure the accuracy of these systems. These identifications are actually being provided by external partners, and it is sometimes the case that "images of innocent people are unnecessarily included as investigative leads" (18).

EFF's extensive testimony also suggested that the burdens imposed by the maldistribution of errors made by these systems will "disproportionately impact people of color" (Lynch, 2017: 2). This outcome is due in part to the "years of well-documented racially-biased police practices" that ensure that all criminal databases will "include a disproportionate number of African Americans, Latinos, and immigrants" (17-18). Arguably, the failures attributed to the use of the FBI's Interstate Photo System stem from the fact that the system does not actually identify a particular individual as the target. Instead, it provides a "ranked list of candidates," which can only ensure that "the candidate will be returned in the top 50 candidates" some 85 percent of the time "when the true candidate exists in the gallery" (10). The FBI argues that this list is only "an investigative lead not an identification," and, as a result, there would actually be no "false positive rate" (10). An additional concern is that many police departments proceed as though the results of 'matches' accomplished even with altered and proxy images are sufficient for use as identifications; this is despite unreported, highly variant rankings of candidate targets (Garvie, 2019).

With support from federal grants, law enforcement agencies have also acquired car mounted license plate readers. Early adopters include sheriff's departments in border states. Like other camera-based systems, these devices often have collection, storage, and analytical resources that capture the date, time and location of the vehicle identified. From this data, on-demand profiles of the vehicles can be generated, including locations frequented and the activities most likely engaged in by the drivers or passengers. The assignment of meaning to, or evaluations of the characteristics of the environments, sites, dates and times from which the data have been gathered is part of the specialized value that computational analysis adds to the so-called raw material camera footage (Cohen, 2017a; Couldry and Mejias, 2019).

The addition of facial recognition technology to BWCs, or to the image processing technology made available for law enforcement as an ancillary service by product vendors, represents a transformative or 'disruptive' enhancement of traditional practices (Owen, 2015). As a form of biometric identification, Facial Recognition Technology (FRT) does not require the subject to be in close proximity to the actors or agents seeking to establish a connection between captured data, and the original source of that data. Gaining access to this kind of 'ground truth' for fingerprints and iris scans generally requires cooperation or, at the very least, awareness on the part of the subject of identification, whereas FRT-based information can be captured and validated from afar, and often without the cooperation and awareness of the target (Nakar and Greenbaum, 2017). At the same time, because identification and comprehensive classifications of individuals, regardless of criminal records, represents a significant threat to privacy and anonymity, many critical observers suggest that police should be required to demonstrate a special need to gather this much information (Nakar and Greenbaum, 2017: 98). However, the rapidly increasing use of FRT for marketing and sales efforts, as well as social and entertainment media applications seems likely to eliminate privacy expectations as a constraint on their use. The technology will be widely available and taken-for-granted (Nakar and Greenbaum, 2017).

While facial recognition is being improved as a capability of surveillance cameras, additional behavioral pattern recognition strategies and techniques are being pursued as a backup for those cases in which facial images are not of sufficient quality for high-confidence identification (Jain, et al., 2016). Evidence suggests that reliable identification of individuals, from captured images in addition to social media commentary and audio-visual recordings of interactions with police officers on street corners or through automobile stops, is bound to improve (Goldenfein, 2018; Joh, 2016; Reid et al., 2013). Additional classificatory aids can be expected to become available following improvements in "automated emotion recognition and classification" (Coudert et al., 2015: 759-760). Such information can also be developed from the analysis of images people share through social media platforms, such as Instagram.

Statistical surveillance

While the technological surveillance described here largely depends upon particular devices, such as cameras and microphones, statistical surveillance relies upon the more generalized resource of powerful computers and high-level data analysis (Cheney-Lippold, 2017). The strategic use of data for the identification and classification of persons, places and things is not new (Bowker and Star, 1999). However, contemporary computational systems can locate, gather and analyze a massive amount of data and put it to use in ways that had only been imagined by the authors of science fiction novels in the past.

A particularly important development is the extent to which usable data are *not* being gathered primarily from highly structured files or databases that have been organized by researchers and analysts to serve particular purposes within the criminal justice system (CJS). Instead, such data are, increasingly, being derived from a variety of environmental sensors, such as those that identify and locate gunshots and suspicious substances (Ferguson, 2018). These surveillance systems have been taught how to make their own sense of the patterns they encounter within the world (Atzori et al., 2010). Statistical surveillance provides 'actionable intelligence' primarily about members of different populations or groups within society that are likely to be evaluated, and then treated differently from members of other identifiable groups. The assignment of individuals to groups identified as gang members, terrorists, or likely victims of crime on the basis of statistical analysis and algorithmic assessment is a routine application of statistical surveillance (Degeling and Berendt, 2018; Ferguson, 2017, 2018).

The use of statistical surveillance by police and other members of the CJS increasingly target groups that are unlikely to have acquired a legal status of the sort afforded to members of other groups that have been granted constitutional protections. Identifying some of the groups to which individuals are said to belong is a matter of tightly held corporate or agency secrecy. Most of us have no knowledge of the groups to which we have been algorithmically assigned. In addition, protections of law in the US are focused primarily upon identifiable individuals, rather than members of idiosyncratically defined groups. Consequently, many of the threats to procedural justice associated with the expansion of statistical surveillance have multiplied while the ability of the law to respond continues to decline (Hildebrandt, 2018).

However, as Barocas and Selbst (2016) remind us, a variety of decisions are made in the collection and processing of available data that also lead to the denial of opportunity and the imposition of constraints upon members of "protected classes." These administrative and procedural actions within the CJS add to the disproportionate burdens that members of these groups already bear. Many disparate impacts that result from the use of algorithmic assessments and recommendations can be explained by the fact that the samples from which data are drawn are not representative of the surrounding populations. While under-representation is the most common source of bias in the data, Barocas and Selbst note that over-representation can also result in unequal attention being paid to members of a group that has been assigned a rating associated with negative stereotypes (Barocas and Selbst, 2016: 686-687).

An additional concern, in regard to the kinds of decisions being made within law enforcement and the management of social welfare programs, is the extent to which the kinds of decisions being made by computer scientists are treating vital public policy issues as engineering or design problems. Kevin Miller (2014) suggests that an early decision about setting initial tolerances for performance in prediction usually involves setting different values and limit levels for positive and negative errors. These are critically important decisions that need to be taken at public, and then administrative agency levels.

Another difficulty is that the values that guide decisions made by commercial vendors, and the engineers who develop their systems, are not likely to match those values that are more common within governments, and among large segments of the public (Brauneis and Goodman, 2018). Considerations of fairness do not usually attract the attention of engineers, yet are among the more challenging requirements for algorithmic systems (Selbst et al., 2019). Of particular interest is the fact that analytical processes used by computational classifiers are not necessarily recognizable variants of the cues or data elements used by human classifiers. And while these systems are

assumed to be capable of processing massive amounts of data, we cannot forget that "predictive models are simplifications that cannot consider all possible relevant facts about subjects, and that therefore necessarily treat people as members of groups, not as individuals" (Brauneis and Goodman, 2018: 123).

For particular groups, the achievement of a particular form of algorithmic fairness is not only meaningful, but highly valued. This places members of the community of "fair-ML practitioners and researchers" in the position of altering distributions of a unique collection of benefits (Selbst et al., 2019: 11). In addition, chosen paths for the articulation and pursuit of fairness standards and strategies of enforcement may not overcome the constraints that a 'business ethics' orientation places on the corporate commitment to ethical design (as opposed to a social justice orientation) (Greene, et al., 2019). In these circumstances, the focus within ongoing ethical debates "is largely limited to appropriate design and implementation—not whether these systems should be built in the first place" (Greene et al., 2019: 2127).

The surveillance economy

It is important to consider the extent to which the development and use of data-based surveillance technology has expanded within the commercial realm (Zuboff, 2015, 2019). However, one must also acknowledge that commercial providers of surveillance-oriented services count government agencies, including the police, among their most reliable and profitable customers. A special concern arises when the corporate providers of essential technology for law enforcement agencies are also the dominant firms in that market. As a result, even large city police departments negotiating the conditions of sale, rental or critical services are at a disadvantage as contract takers rather than as negotiators. Here, it is not so much the devices, such as fixed and mobile cameras, which are expensive, but the specialized cloud-based data management services, which also require long-term high value contracts (Gelles, 2016; Joh, 2017). The special relationships that are imposed upon the police agencies as contract takers often leaves their officials without a detailed understanding of the extent to which they actually own, and control the use of the data that their surveillance systems generate. This uncertainty means that these private companies are able to "exert an undue influence" that can "affect legal change, police oversight, and police accountability" (Joh, 2017: 120). A dominant leader in the manufacture and marketing of body-worn cameras (BWCs) is Axon, previously known as Taser International, primarily for its popular stun guns (Joh, 2019). When Axon acquired its major competitor VIEVU in May 2018, it owned "80% of all big-city police department contracts" (Duprey, 2018). Axon has also recently solidified its influence over the development and marketing of associated services for the management of data generated by its cameras (Gelles, 2016; Greene and Patterson, 2018). The uses to which Axon will put the data that it manages for police departments are also concerning. For example, it is reported that Axon will use the massive amounts of video it stores for its clients to train their AI systems. This will reduce the time and effort that police officers, and perhaps even prosecutors and judges expend to make efficient and effective use of that data for routine tasks (Greene and Patterson, 2018). Elizabeth Joh (2019: 2) argues that a marketplace dominated by a single corporation means that police agencies "have little choice and input into the final product procured." More critical still, is the fact that police "agencies were purchasing and investing in a *platform*, not just individual machines" (Joh, 2019: 3). Joh (2019: 4) notes that data management services are the real source of both profits and influence being exercised by Axon. This includes not just cloud data storage based

upon its Evidence.com platform, but also the software management systems that allow agencies to secure remote access, tag metadata and utilize services such as redaction and transcription. The fact that Axon offered their cameras for free for a year, while charging for the data management services, demonstrates the importance of the platform. The expansion of platform services being developed by Axon shows the capacity of the system to integrate the collection and processing of data in ways that are likely to accelerate the deskilling of police officers. One concerning proposal is the enhancement of the "records management system" so as to "reduce the time officers spend writing reports." According to an executive vice-president of Axon's Worldwide Products: "One day we will be able to have AI work on BWC video and in-car video to create a first draft of a report that an officer can go into and edit." In addition, records "are automatically connected to reduce the amount of time cops spend filling out paperwork so they can get back on the street. That is our mission." (Perry, 2018).

Although the same level of market dominance in the predictive and analytic technologies used within the criminal justice system (CJS) is not evident, there are some firms that are especially important because of their connections with the police and other government agencies. Perhaps the most important of these is Palantir, a specialist in data analytics and a provider of predictive policing technology that owes much of its early success to contracts with the US Central Intelligence Agency (Shapiro, 2019; Sloan and Warner, 2016; Waldman et al., 2018). As law enforcement agencies become active users of commercial sources of privately collected data, such as that derived from social media, they bypass constitutional limits that would constrain their own gathering of that information (Brayne, 2017). Early criticisms of Palantir's ethical shortcomings were focused on its involvement in helping "Cambridge Analytica use the personal data of up to 87 million Facebook users to develop psychographic profiles of individual voters" (Waldman et al, 2018: 6). Palantir's success in monetizing data for corporations is not yet matched by its provision of services for police departments (these often involve training officers to use its products like Foundry and Gotham as resources accessible through 'fusion centers'). Still, Palantir's growth in this area has been dramatic. Gotham is not a stand-alone device but is primarily used as resource through which "human and computational agents working together... assist a human analyst in discovering key signals in a sea of big data noise" (Munn, 2017: 2). However, critical analyses from a technical perspective call attention to troublesome distinctions between "algorithmic proximity" and "geographical proximity." Further, the representation of relations between people on an analyst's screen may not mesh well with the notions of proximity that system users normally rely upon (Munn, 2017: 6).

The Los Angeles Police Department (LAPD) used Gotham to "identify and deter people likely to commit crimes". Lists developed from the analysis of data from multiple sources are "distributed to patrolmen, with orders to monitor and stop the pre-crime suspects as often as possible, using excuses such as jaywalking or fix-it-tickets." Field interview cards generated from these interventions "are digitized in the Palantir system, adding to a constantly expanding surveillance database that's fully accessible without a warrant" (Waldman et al., 2018: 11). The constitutional concerns raised by this process are hard to ignore, and pathways through the CJS for the targeted groups lead increasingly toward more time behind bars. The Palantir system for the automated license plate reader (ALPR), developed for use by the LAPD, generally performs quite well. But, when it makes a mistake, its victims are often members of "groups already marginalized or vulnerable." One especially worrisome example of the kinds of errors that are possible involved a misreading of a license plate number, whereupon police were mobilized to pull over an African

American woman because her car had been flagged as stolen. She was ordered out of her car and forced to her knees at gunpoint. She waited in handcuffs until police completed searching her car (Munn, 2017:10). It does not take much to imagine how this interaction might have turned out, and the data are not at all encouraging (Johnson, et al., 2018).

A third major actor in this rapidly developing market in surveillance technology is Vigilant Solutions (VS). They are known primarily for services delivered to law enforcement agencies, centered around their ALPRs (Joh, 2016) and related services enabled through analysis of available databases. VS has also been identified as a prime example of "platform policing: the implementation of cloud-based platforms, built and run by private companies, that provide mass surveillance-driven simulations for a range of police operations, including predictive policing" (Linder, 2019: 76). VS' platform, Vigilant Investigative Centre (VIC), "fuses mass surveillance data from diverse private, public, and state sources". The data is transformed through "an array of data analytics to law enforcement" (Linder, 2019: 77). This multisectoral global enterprise is a prime example of what has been characterized as a "surveillant assemblage" (Haggerty and Ericson, 2000). A variety of partners share VIC resources, while also sharing the data from their own activities (which VIC is also monetizing). The integration and sharing of data is being reinforced economically by the network effects that make it difficult for users to limit their reliance on services and capabilities that have become normative (Couldry and Mejias, 2019).

Cumulative assessment

Motivated by the engaged efforts of communication and information scholars, such as Christian Sandvig, data scientists, such as Solon Barocas and Andrew Selbst, and social theorists, including Mireille Hildebrandt, this article has explored the development, application and critical evaluation of algorithmic technologies within the criminal justice system (CJS). Although the entire CJS system is administratively, bureaucratically and jurisdictionally complex, my primary focus has been on the use of these technologies by police officers in large and mid-sized cities in the United States. There has been a transformational effect on the nature of policing such that deskilling is an appropriate label for the changes taking place. The impact of these technologies on members of poor and minority communities is not so easily categorized. There is little doubt, however, that the effects are greater for them than for other segments of the population.

Understanding the impact of algorithmic technologies, including those used in the processing of audiovisual data being captured by body-worn cameras (BWCs), as well as the massive data accessed from remotely networked platforms, is becoming a nearly insurmountable challenge. Limitations on access to the data, and the increasingly complex analytics that transform it into actional intelligence, make evaluative assessments of its biases, errors and the distribution of consequences difficult to characterize in generalizable terms. A variety of factors are associated with limitations on access. Not the least of these is the growing complexity of the rapidly changing computational routines applied by algorithms within devices and by the networks that distribute general, and highly specialized assessments and recommendations. Complex processes become difficult to understand, while recommendations, or even behaviorally pre-emptive decisions, become increasingly clear but unchallenged.

While it is important to understand the nature of the algorithmic processes that are used in generating recommendations, it is also crucial to understand how the goals, and procedural standards that guide their pursuit are established. Although it seems clear that engineers and

technicians need to have some understanding of how particular outcomes are produced algorithmically, there is considerable uncertainty about how the general public and their legislative and administrative agents should determine those outcomes. There is what many consider to be an even more important determination, for which the involvement of the public seems likely to have been further marginalized. This concerns the relationships between false positives and false negatives that differ so substantially across time, space and population. The public role in these critical decisions associated with transparency and accountability largely depends on their access to and understanding of the data which informs those decisions.

Limitations on access to both data and analytics arise from assertions of property rights, only some of which are expressed formally within the law. Others are hidden within the service agreements that accompany the establishment of relationships between devices and the services that enable them to perform their myriad functions. The ability of service providers to establish and enforce their restrictive policies is based to a large extent on their market power, and the rapidly advancing sense that those particular services are actually necessities, rather than options. Firms such as Axon and Palantir have established dominant positions within the markets for law enforcement goods and services. They are able to establish their own policies regarding the provision of particular capabilities in the systems they make available. While Axon appears to have followed the lead of progressive cities like San Francisco in barring the use of facial recognition with BWCs, it is making its own rules about how the data derived from its cameras in the field will be used to develop other law enforcement services.

Given the importance of public involvement in determining the rules governing the use of algorithmic systems within the CJS, this article will conclude with an assessment of some domestic projects which are seeking to improve the standards and practices of algorithmic accountability. It is to be hoped that domestic and international agencies will be given responsibility to increase our understanding of, and influence over, the development and use of these systems within the CJS and other societal domains.

The policy horizon

So, what is to be done? While Couldry and Mejias (2019) identity the appropriation of data, or TGI as a new stage in the development of capitalism, they see the recognition of this development as a pre-requisite for establishing the kinds of resistance that the circumstances demand. Zuboff (2019) suggests that rather than a variant of colonialism, we should understand surveillance capitalism as something akin to a "coup from above, not an overthrow of the state, but rather an overthrow of the people's sovereignty." She calls for the mobilization of "new forms of collaborative action" (21). We need to identify the damage that has been done to us, individually and collectively, and reclaim our rights to the knowledge collected from us and about us as a resource for our liberation.

As we are developing that knowledge, it seems clear that, as Hildebrandt (2018) has suggested, criminal justice systems around the globe have to be brought under control through the rule of law. Its degradation by corporate actors will need to be contested. It is not obvious that this contestation will focus upon the meaning of social justice and inequality, but there are good reasons for making it so. Jonathan Cinnamon invites us to consider Nancy Fraser's three "obstacles to parity of participation", especially "maldistribution" and "misrecognition". These formulations align with the problems associated with algorithmic decision-making within the CJS (Cinnamon, 2017: 613).

Public interest and advocacy organizations have attempted to modify the behavior of the CJS through court interventions and the mobilization of public opinion. In 2016, the American Civil Liberties Union (ACLU) initiated a Community Control Over Police Surveillance (CCOPS) effort in order to mobilize demand for laws that would increase the public's influence over decisions regarding the use of surveillance technologies within their communities. The following year, they developed and distributed a model bill for passage by city councils around the nation (ACLU, 2018). The fact that eight cities had already passed bills incorporating many of the guiding principles behind their draft legislation, with an additional 20 cities and two states (California and Maine) engaged in the development of their own versions, suggests that the ACLU's initiative was both timely and well developed (ACLU, 2018). In 2019, San Francisco led the way in banning the police use of facial recognition technology, despite claims by the Police Officer's Association that "the ban would hinder their members' efforts to investigate crime" (Conger et al., 2019).

The Electronic Frontier Foundation's (EFF) senior staff attorney, Jennifer Lynch provided a comprehensive list of proposals for the kinds of legislation that might help to reduce the burdens on poor and minority group members from "over-collection of face recognition data," and the "current uncertainty of Fourth Amendment jurisprudence" in this area (Lynch, 2017: 23-26). The proposals include an engagement with the dangers that flow from the combination of multiple databases, including the merging of biometrics with a variety of contextual data in ways likely to widen the nature and extent of privacy harms. Their final recommendation addressing the absence of a privacy commission in the US declares that government "entities that collect or use face recognition must be subject to meaningful oversight from an independent entity." The fact that Axon, the dominant provider of body worn cameras for police use has followed the advice of its own independent ethics board by deciding that they "would ban the use of facial recognition systems on its devices" (Warzel, 2019), suggests that acceptance of independent assessments is spreading.

The Leadership Conference on Civil and Human Rights and Upturn, a Washington, DC nonprofit entity, have developed a different set of policies and practices that they believe should be adopted by the nation's police departments (Yu et al., 2017). In 2017, they evaluated 75 local police departments nationwide, focusing their attention on the major city departments, as well as those that had received significant grants from the Department of Justice to support their camera programs.

Eight criteria derived from their "Civil Rights Principles on Body Worn Cameras" were graded on the extent to which department policies needed to satisfy those criteria. Among the eight evaluative criteria used in this scorecard, those with particular relevance to questions being raised by members of the most recorded populations concerned whether policies: 1) limited officer discretion on when to record; 2) addressed personal privacy concerns; 3) prohibited officer pre-report viewing; 4) protected footage against tampering and misuse; 5) made footage available to individuals filing complaints; and 6) limited biometric searching of footage (Yu et al., 2017: 6-7). Not all of the frequently expressed public concerns about the use of BWCs were included among these eight criteria (Zwart, 2018). One major blind spot is that access to recordings are restricted to police and prosecutors. This places criminal defendants at a significant procedural disadvantage. The EFF did note, however, that none of the department policies they evaluated had a "blanket limitation on officer review of footage before filing an initial written incident report." They also reported that the "vast majority of departments (55) allow officers unrestricted footage review." (Yu et al., 2017: 8-9).

The efforts of the ACLU, the Leadership Forum, Upturn and EFF will need to be expanded, and replicated at local, state, national and international levels. Independent agencies are needed to

advance recommendations for establishing regulatory limits on the misappropriation and exploitation of TGI and other forms of data being used in the management of the global CJS. These recommendations should be based on research that evaluates and compares different systems as they are used within different agencies and departments. Evaluations would hopefully focus on the nature and extent of the bias and error that are common within applications. For those population segments already burdened with disadvantage, parity in participation within national and local levels of governance that we associate with the management of both positive and negative errors would need to be identified. And finally, the reconstitution of an agency with a public policy mission like that of its predecessor, the US Office of Technology Assessment, would be an essential step toward overcoming an addiction to technological developments that threaten, rather than advance the human condition (Graves and Kosar, 2018).

At the international level, the equivalent of the Intergovernmental Panel on Climate Change needs to be developed to confront the mounting threats to democracy arising from the development of automated surveillance. It should be noted that the United Nations Office of the High Commissioner for Human Rights includes "enhancing participation and protecting civic space" among its priorities. Its Management Plan for 2018-2021 includes a focus on "[d]igital space and emerging technologies" noting that "[u]nequal access to technologies and increasingly powerful algorithms contribute significantly to discrimination and inequality" (United Nations, 2018: 44). The development of such an international effort focused on addressing the global impact of automated surveillance technology is an important step forward that needs to be taken while there is still time.

Author Bio

Oscar Gandy is an emeritus professor of communication who retired from active teaching in 2006. His research and teaching were in the area of political economy with an emphasis on media institutions, communication and race, privacy and surveillance, and communication and information policy. An active scholar before and after his retirement, Professor Gandy has published in excess of 80 articles and chapters and authored four well-received books (*Beyond Agenda Setting*, *Communication and Race*, *The Panoptic Sort* and *Coming to Terms with Chance*).

Acknowledgements

An earlier version of this article was delivered in the Law Section at the IAMCR in Madrid, Spain, 8 July 2019.

References

ACLU (2018) *An act to promote transparency, the public's welfare, civil rights, and civil liberties in all decisions regarding the funding, acquisition, and deployment of military and surveillance equipment*. Model bill with comments. Available at: https://www.aclu.org/sites/default/files/field_document/aclu_ccopsm_model_bill_october_2018.pdf (accessed 18 July 2019).

Ananny M and Crawford K (2016) Seeing without knowing: limitations on the transparency ideal and its application to algorithmic accountability. *New Media & Society* 20(3): 1-17.

Andrejevic M (2019) Automating surveillance. *Surveillance & Society* 17(1/2): 7-13.

Ariel B, Farrar WA and Sutherland A (2015) The effect of police body-worn cameras on the use of force and citizens' complaints against the police: a randomized controlled trial. *Journal of Quantitative Criminology* 31(3): 1-27.

Atzori L, Iera A and Morabito G (2010) The internet of things: a survey. *Computer Networks* 54(15): 2787-2805.

Barocas S and Selbst AD (2016) Big data's disparate impact. *California Law Review* 104: 671-732.

Bedoya A (2017) *Statement of Alvaro Bedoya, Executive Director, Center on Privacy & Technology at Georgetown Law*. Hearing on Law Enforcement's Use of Facial Recognition Technology. Washington, DC: US House of Representatives Committee on Oversight and Government Reform.

Berman E (2018) A government of laws and not of machines. *Boston University Law Review* 98: 1277-1355.

Beutin LP (2017) Racialization as a way of seeing: the limits of counter-surveillance and police reform. *Surveillance & Society* 15(1): 5-20.

Binns R (2018) Algorithmic accountability and public reason. *Philosophy and Technology* 31(4): 543-556.

Blount K (2017) Body worn cameras with facial recognition technology: when it constitutes a search. *Criminal Law Practitioner* III(IV): 61-81.

Bollier D (2018) *Artificial Intelligence, The Great Disruptor: Coming to Terms with AI-driven Markets, Governance and Life*. Report. Washington, DC: The Aspen Institute. Available at: http://csreports.aspeninstitute.org/documents/AI2017.pdf (accessed 18 July 2019).

Bowker GC and Star SL (1999) *Sorting Things Out: Classification and its Consequences*. Cambridge, MA: The MIT Press.

Brauneis R and Goodman EP (2018) Algorithmic transparency for the smart city. *Yale Journal of Law & Technology* 20: 103-176.

Brayne S (2017) Big data surveillance: The case of policing. *American Sociological Review* 82(5): 977-1008.

Browne S (2015) *Dark Matters: On the Surveillance of Blackness*. Durham, NC: Duke University Press.

Burrell J (2016) How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society* (January-June): 1-12.

Campolo AM, Sanfilippo M, Whittaker M et al. (2017) *AI Now Report 2017*. New York: AI Now Institute at New York University.

Caplan R, Donovan J, Hanson L et al. (2018) *Algorithmic Accountability: A Primer*. NY: Data & Society Research Institute. Accessible at: https://datasociety.net/?s=Algorithmic+Accountability%3A+A+Primer (accessed 24 October 2019).

Chen CF (2017) Freeze, you're on camera: Can body cameras improve American policing on the streets and at the borders? *University of Miami Inter-American Law Review* 48(3): 141-187. Available at: http://repository.law.miami.edu/umialr/vol48/iss3/7 (accessed 24 October 2019).

Cheney-Lippold J (2017) *We are Data: Algorithms and the Making of Our Digital Selves*. New York: New York University Press.

Cinnamon J (2017) Social Injustice in Surveillance Capitalism. *Surveillance & Society* 15(5): 609-625.

Cino JG (2018) Deploying the secret police: the use of algorithms in the criminal justice system. *Georgia State University Law Review* 34(4): 1073-1102. Available at: https://readingroom.law.gsu.edu/gsulr/vol34/iss4/6 (accessed 13 October 2019).

Citron DK (2008) Technological due process. *Washington University Law Review* 85(6): 1249-1313.

Cohen JE (2017a) Law for the platform economy. *U.C. Davis Law Review* 51: 133-204.

Cohen JE (2017b) Surveillance vs. privacy: effects and implications. In: Gray D and Henderson SE (eds). *Cambridge Handbook of Surveillance Law*. New York: Cambridge University Press, pp. 455-469.

Conger K, Fausset R and Kovaleski SF (2019) San Francisco bans facial recognition technology. *New York Times* (14 May). Available at: https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html (accessed 18 July 2019).

Coudert F, Butin D and Metayer DL (2015) Body-worn cameras for police accountability: opportunities and risks. *Computer Law & Society Review* 31: 749-762.

Couldry N and Mejias UA (2019) *The Costs of Connection: How Data is Colonizing Human Life and Appropriating it for Capitalism*. Stanford, CA: Stanford University Press.

Degeling M and Berendt B (2018) What's wrong about robocops as consultants? A technology-centric critique of predictive policing. *AI & Society* 33(3): 347-356.

Duprey R (2018) Axon enterprise now owns the police body cam market. Motley Fool Available at: https://www.fool.com/investing/2018/05/18/is-there-any-stopping-axon-enterprise-now.aspx (accessed 10 October 2019).

Eubanks V (2018) *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. NY: St. Martin's Press.

Ferguson AG (2012) Predictive policing and reasonable suspicion. *Emory Law Journal* 62: 259-325.

Ferguson AG (2015) Big data and predictive reasonable suspicion. University of *Pennsylvania Law Review* 163(2): 327-410.

Ferguson AG. (2017) Policing predictive policing. *Washington University Law Review* 94(5): 1115-1194.

Ferguson AG (2018) Illuminating black data policing. *Ohio State Journal of Criminal Law* 15: 503-525.

Ferguson AG (2019) The exclusionary rule in the age of blue data. *Vanderbilt Law Review* 72(2): 561-645.

Frameworks Institute (2019) *Unleashing the Power of How: An Explanation Declaration*. Washington, DC: The Frameworks Institute.

Fussell S (2018) The always-on police camera (26 September). *The Atlantic*. 28 September. Accessible at: https://www.theatlantic.com/technology/archive/2018/09/body-camera-police-future/571402/ (accessed 27 October 2019).

Fussey P and Murray D (2019*) Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*. Colchester, UK: University of Essex, Human Rights Center.

Gandy OH Jr (2009) *Coming to Terms with Chance: Engaging Rational Discrimination and Cumulative Disadvantage*. Burlington, VT: Ashgate Publishing.

Gandy OH Jr (2012) Statistical surveillance: remote sensing in the digital age. In: Ball K, Haggerty KD and Lyon D (eds*). Routledge Handbook of Surveillance Studies*. New York: Routledge, pp. 125-132.

Garvie C (2019) *Garbage in, Garbage out. Face recognition on flawed data.* Georgetown Law, Center on Privacy & Technology (16 May). Available at: https://www.flawedfacedata.com (accessed 18 July 2019).

Garvie C and Moy LM (2019) *America under Watch: Face Surveillance in the United States*. Report. Washington, DC: Center on Privacy & Technology, Georgetown University Law Center. Available at: https://www.americaunderwatch.com (accessed 28 October 2019).

Gelles D (2016) Taser International dominates police body camera market. *New York Times*, 14 July, Section B, p. 1.

Goel S, Perelman M and Shroff R et al. (2017). Combatting police discrimination in the age of big data. New *Criminal Law Review* 20(2): 181-232.

Goldenfein J (2019) The Profiling Potential of Computer Vision and the Challenge of Computational Empiricism. *Proceedings of the 2019 ACM FAT* Conference*, forthcoming. Available at: https://ssrn.com/abstract=3284598 (accessed 27 October 2019).

Graves Z and Kosar K (2018) *Bring in the Nerds: Reviving the Office of Technology Assessment*. R Street Policy Study No. 128. R Street Institute. Available at: https://www.rstreet.org/wp-content/uploads/2018/01/Final-128.pdf (accessed 14 October 2019).

Greene D and Patterson G (2018) Can we trust computer with body-cam video? Police departments are being led to believe AI will help, but they should be wary. *IEEE Spectrum* 55(12). Available at: https://ieeexplore.ieee.org/abstract/document/8544982 (accessed 28 October 2019).

Greene D, Hoffman AL and Stark L (2019) Better, Nicer, Clearer, Fairer: A Critical Assessment of the Movement for Ethical Artificial Intelligence and Machine Learning. *52nd Hawaii International Conference on System Sciences*, Hawaii. Available at: http://hdl.handle.net/10125/59651 (accessed 18 July 2019).

Haggerty KD and Ericson RV (2000) The surveillant assemblage. *British Journal of Sociology* 51(4): 605-622.

Hildebrandt M (2018) Law as computation in the era of artificial legal intelligence: speaking law to the power of statistics. *University of Toronto Law Journal* 68(1):12-35.

Hu M (2017) Algorithmic Jim Crow. *Fordham Law Review* 86(2): 633-696.

Hung V, Babin S and Coberly J (2016) A Primer on Body Worn Camera Technologies. Laurel, MD: John Hopkins University Applied Physics Laboratory.

Jain AK, Nandakumar K and Ross A (2016) 50 years of biometric research: accomplishments, challenges, and opportunities. *Pattern Recognition Letters* 79(1): 80-105. Available at https://doi.org/10.1016/j.patrec.2015.12.013 (accessed 22 October 2019).

Joh EE (2016) The new surveillance discretion: automated suspicion, big data and policing. *Harvard Law & Policy Review* 10: 15-42.

Joh EE (2017) The undue influence of surveillance technology companies on policing. *New York University Law Review* 92: 101-130.

Joh EE (2019) Police surveillance machines: a short history. *Law and Political Economy*, forthcoming. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3218483 (accessed 10 October 2019).

Johnson O, Gilbert K and Ibrahim H (2018) *Race, Gender and the Contexts of Unarmed Fatal Interactions with Police*. Fatal Interactions with Police Study. St Louis, MO. Available at: https://cpbusw2.wpmucdn.com/sites.wustl.edu/dist/b/1205/files/2018/02/ (accessed 29 October 2019).

Kaufmann S (2016) Security through technology? Logic, ambivalence and paradoxes of technologized security. *European Journal of Security Research* 1(1):77-95.

Linder T (2019) Surveillance capitalism and platform policing: The surveillant assemblage-as-a-service. *Surveillance & Society* 17(1/2): 76-82. Available at: https://ojs.library.queensu.ca/index.php/surveillance-and-society/index (accessed 23 October 2019).

Lynch J (2017) *Testimony*. Hearing on Law Enforcement's Use of Facial Recognition Technology. United States House Committee on Oversight and Government Reform. Washington, DC: Electronic Frontier Foundation.

Lyon D (2003) Surveillance as social sorting: computer codes and mobile bodies. In: Lyon D (ed) *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*. New York: Routledge: 13-30.

Mateescu A, Rosenblat A and Boyd D (2015) *Police Body-Worn Cameras*. NY: Data & Society Research Institute. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2569481 (accessed 28 October 2019).

Mateescu A, Rosenblat A and Boyd D (2016) Dreams of accountability, guaranteed surveillance: the promises and costs of body-worn cameras. *Surveillance & Society* 14(1): 122-127. Available at: https://ojs.library.queensu.ca/index.php/surveillance-and-society/index (accessed 24 October 2019).

Maurer D (2017) *Face Recognition Technology: DOJ and FBI Need to Take Additional Actions to Ensure Privacy and Accuracy*. Testimony. House Committee on Oversight and Government Reform. U. S. Government Accountability Office, GAO-17-489T.

McCluskey JD, Uchida CD, Solomon SE, Wooditch, A, Connor, C, and Revier, L (2019) Assessing the effects of body worn cameras on procedural justice in the Los Angeles Police Department. *Criminology* 57(2): 208-236. Available at: https://onlinelibrary.wiley.com/doi/abs/10.1111/1745-9125.12201 (accessed 24 October 2019).

Miller K (2014) Total surveillance, big data, and predictive crime technology: privacy's perfect storm. *Journal of Technology Law & Policy* 19: 105-146.

Moses LB and Chan J (2018) Algorithmic prediction in policing: assumptions, evaluation and accountability. *Policing and Society* 28(7): 806-822.

Munn L (2017) Seeing with software. Palantir and the regulation of life. *Studies in Control Societies*. Available at: https://researchdirect.westernsydney.edu.au/islandora/object/uws:41249/datastream/PDF/ (accessed 10 October 2019).

Nakar S and Greenbaum D (2017) Now you see me. Now you still do: facial recognition technology and the growing lack of privacy. *Boston University Journal of Science & Technology Law* 23: 88-123.

Obama B (2017) The president's role in advancing criminal justice reform. *Harvard Law Review* 130: 811-866.

Owen T (2015) *Disruptive Power: The Crisis of the State in the Digital Age*. Oxford: Oxford University Press.

Palmer D (2016) The mythical properties of police body-worn cameras: a solution in search of a problem. *Surveillance & Society* 14(1): 138-144.

Perry N (2018) How Axon is accelerating tech advances in policing. *PoliceOne.com News*. Available at: https://www.policeone.com/police-products/body-cameras/articles/how-axon-is-accelerating-tech-advances-in-policing-ZthVdQf8A0cWl8Ax/ (accessed 10 October 2019).

Ratcliffe JH, Taniguchi T and Taylor RB (2009) The crime reduction effects of public CCTV cameras: a multi-method spatial approach. *Justice Quarterly* 26(4): 747-770.

Reid DA, Samangooei S, Chen C, Nixon, M.S., Ross A (2013) Soft biometrics for surveillance: an overview. In: Rao CR and Govindaraju V (eds*) Handbook of Statistics: Machine Learning: Theory and Applications*, Vol 31: 327-353. Available at https://www.sciencedirect.com/science/article/pii/B9780444538598000138 (accessed 22 October 2019).

Rieke A, Bogen M and Robinson DG (2018). *Public Scrutiny of Automated Decisions: Early Lessons and Emerging Methods*. Report. Washington, DC: Upturn, and Omidyar Network.

Sacharoff L and Lustbader S (2017) Who should own police body cameras? Washington *University Law Review* 95(2): 267-323.

Sandvig C, Hamilton K and Karahalios K and Lanbort C (2016) When the algorithm itself is a racist: diagnosing ethical harm in the basic components of software. *International Journal of Communication* 10: 4972-4990.

Selbst AD, Boyd D and Friedler SA, Venkatasubramanian S and Vertesi J (2019) Fairness and abstraction in sociotechnical systems. *2019 ACM Conference on Fairness, Accountability, and Transparency*. Available at: https://doi.org/10.1145/3287560.3287598 (accessed 18 July 2019).

Shapiro A (2019) Predictive policing for reform? Indeterminacy and intervention in big data policing. *Surveillance & Society* 17(3/4): 456-472.

Sloan RH and Warner R (2016) The self, the Stasi, the NSA: privacy, knowledge and complicity in the surveillance state. *Minnesota Journal of Law, Science & Technology* 17(1): 347-408.

Slobogin C (2002) Public privacy: camera surveillance of public places and the right to anonymity. *Mississippi Law Journal* 72: 213-315.

Smykla JO, Crow MS, Crichlow VJ et al (2016) Police body-worn cameras: perceptions of law enforcement leadership. *American Journal of Criminal Justice* 41: 424-443.

Squillacote R and Feldman L (2018) Police abuse and democratic accountability: agonistic surveillance of the administrative state. In: Bonner MD, Seri G, Kubal MR and Kempa M (eds) *Police Abuse in Contemporary Democracies.* Palgrave/Macmillan: Switzerland, pp. 135-164.

United Nations Human Rights Office (2018) United Nations Human Rights Management Plan, 2018-2021. Geneva, Switzerland: United Nations Human Rights Office. Available at: https://www2.ohchr.org/english/OHCHRReport2018_2021/OHCHRManagementPlan2018-2021.pdf (accessed 14 October 2019).

Van Brakel R and De Hert P (2011) Policing, surveillance and law in a pre-crime society: understanding the consequences of technology based strategies. *Cahiers Politiestudies Jaargang* 3(20):163-192.

Waldman P, Chapman L and Robertson J (2018). Palantir knows everything about you. Bloomberg Business Week, 19 April. Available at: https://www.bloomberg.com/features/2018-palantir-peter-thiel/ (accessed 10 October 2019).

Warzel C (2019) A major police body cam company just banned facial recognition. *New York Times*. 27 June. Available at: https://www.nytimes.com/2019/06/27/opinion/police-cam-facial-recognition.html (accessed 20 October 2019).

Weisburd D and Majmundar MK (eds) (2017) *Proactive Policing: Effects on Crime and Communities.* National Academies of Sciences, Engineering, and Medicine. Washington, DC: National Academies Press.

Wenner J (2016) Who watches the watchmen's tape? FOIA's categorical exemptions and police body-worn cameras. *University of Chicago Legal Forum* 2016: 873-906.

White MD and Fradella HF (2018) The intersection of law, policy, and body-worn cameras: an exploration of critical issues. *North Carolina Law Review* 96: 1580-1638.

Wood SE (2017) Police body cameras and professional responsibility: public records and private evidence. *Preservation, Digital Technology & Culture* 46(1): 41-51.

Yokum D, Ravishankar A and Coppock A (2017) *Evaluating the Effects of Police Body-Worn Cameras. A Randomized Controlled Trial*. Working Paper. Washington, DC: The Lab @ DC. Available at: https://bwc.thelab.dc.gov/TheLabDC_MPD_BWC_Working_Paper_10.20.17.pdf (accessed 14 October 2019).

Yu C, Cook S, Paluch L, Yu H and Bogen M (2017) *Police Body Worn Cameras: A Policy Scorecard*. Washington, DC: The Leadership Conference on Civil and Human Rights.

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

Zuboff S (2019) *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. NY: Public Affairs.