The Algorithm made me do it!

Predictive policing, cameras, social media and affective assessment

Oscar H. Gandy, Jr.
Annenberg School for Communication
University of Pennsylvania
oscar.gandy@asc.upenn.edu

Law Section
OCS 19590

Paper presented at the IAMCR 2019 conference in
Madrid, Spain, July 7-11, 2019

Abstract

Christian Sandvig and his colleagues (2016) helped to set the research agenda for communication and information scholars concerned about the impact of algorithmic techniques for the generation of 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 & Selbst, 2016). Attention to the impact of these systems has just begun to be developed with regard to the challenges associated with the law, and its defense of the fundamental rights of members of those groups. This paper 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 (Kroll, et al., 2017; van Brakel & De Hert, 2011; Whittaker, et al., 2018; Winston, 2018).

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 (McPhail, B. and A. Clement, et al., 2013). Increasingly, however, the work of human monitors has been re-assigned to semi-autonomous computer systems, guided by artificial intelligence resources, updated routinely through the use of machine learning techniques (Berman, 2018; Mateescu, et al., 2015; Sackler and Sackler, 2017). The use of cameras, especially those by officers on foot patrol, or in motor vehicles is described, but a primary focus of this paper is on the computer-aided analysis of the images captured by these devices.

The capture and use of images from mobile cameras, the analysis of social networks as well as affective assessments of individuals and members of groups derived from automated analysis of social media text and images, as well as other transaction-generated information (TGI) that has come to be referred to as "big data," has been recognized as contributing to the development of a transformative moment in the nature of policing (Brayne, 2017; Degeling and Berendt, 2017; Hu, 2017; Manovich, 2018). The application of these and other informational resources to the development of predictive policing has been recognized as presenting a genuine threat to the traditional meaning of "reasonable suspicion" and related justifications for the application of First, Fourth, Fifth and Fourteenth Amendment rights to the targets of police attention (Cohen, 2019; Ferguson, 2015, 2016; Maharrey, 2018).

This paper will explore these developments, with special regard to their likely impact upon the life chances, well-being, and social construction of members of racialized population segments in the foreseeable future (Carney & Enos, 2017; Turow and Hennessy, et al., 2018).

Introduction

Christian Sandvig and his colleagues (2016) helped to set the research agenda for communication and information scholars concerned about the impact of algorithmic techniques

for the generation of 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 & Selbst, 2016). Attention to the impact of these systems has just begun to be developed with regard to the challenges associated with the law, and its defense of the fundamental rights of members of those groups. This paper 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 (Kroll, et al., 2017; van Brakel & De Hert, 2011; Whittaker, et al., 2018; Winston, 2018).

Mireille Hildebrandt (2018) identifies her efforts in a recent paper as seeking to promote the "concept and practice of 'legal protection by design'" that she believes "may contribute to sustaining law as meaningful information that informs the consequences of our actions, seeking to bring artificial legal intelligence under the Rule of Law" (p. 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.

I am pleased to align the efforts being made in this paper with those goals, especially as they apply to the members of the criminal justice systems around the world whose daily routines are being radically altered by their increased reliance on artificial intelligence (AI) devices, systems and services, that are almost continually being updated through machine learning (ML). Although there are good reasons for considering the impact of these developments on the quality of the work-life enjoyed by the members of the CJS, our focus is on the consequences that flow from the interactions between these laborers within the legal system and those members of society whose behavior they seek to regulate or bring under control.

Hildebrandt (2018) identifies four attributes of reliance on artificial legal intelligence that she suggests may "disrupt the concept and the Rule of Law": 1) the inaccessibility of the software used in rendering decisions may make them "inscrutable and thereby incontestable"; 2) "the shift from meaningful information to computation entails a shift from reason to statistics, and from argumentation to simulation"; 3) "a set of fundamental rights may be infringed, compromised or even violated"; and 4) "to the extent that the algorithms become highly proficient… lawyers may outsource part of their work" with the result of their becoming increasingly deskilled, including the loss of their ability "to check whether the software 'gets it right', confronting us with a new Catch22" (pp. 11-12).

This paper will begin with an examination of the role played by information and communication technology (ICTs) in the identification, classification, prediction, evaluation and proscriptive recommendations being provided to decision-makers within the CJS. Focusing primarily on cameras and associated audiovisual technologies with fixed and mobile installations, this initial review will emphasis the usage of these systems to provide biometric identification and affective assessments. An important part of the technology that enables the work beginning with identification is mathematical, or computational. The fact that large part of the computation that identifies us as individuals, as well as members of groups makes use of massive amounts of

transaction-generated-information (TGI), only a fraction of which actually is generated by the individual whose image has been captured by a camera or other environmental sensor. This process of remote sensing, that we can think of as statistical surveillance, is becoming more and more powerful through developments in artificial intelligence and machine learning. And we'll move fairly quickly through an examination of the nature of the surveillance economy, taking note of some of the attributes of this technology, the work it does with regard to data management through the network interconnections some refer to as "the cloud," and calling attention to the special character of this 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 who struggle to gain access to the data that determines the quality of life that they, their families, and their communities will get to enjoy. Understanding how these systems affect the quality of life for so many requires us to consider the challenges to traditional policing that are being confronted on a daily basis. Some of these challenges are based on rising concerns being expressed about the accuracy, as well as the bias and fairness of these algorithmic systems as they are shaping decisions throughout the CJS. Many of these concerns relate to consequences that flow from the adoption of predictive policing as a spatially, as well as an individually focused strategy.

These new strategies demand continual reassessment of standards for the assessment of reasonable suspicion before decisions are made about whether to stop and search a pedestrian, or someone standing on a street corner. They also affect the management of evidence, and the exclusionary rules that determine whether information generated through the analysis of massive data gathered remotely, can be introduced within a variety of proceedings. All of these assessments play an increasingly important role in determining how transparency and accountability shape the relationships between the police, the courts, and the communities they are supposed to serve.

Following that extensive, but still limited review of the challenges to policing, we'll make a shift in focus to consider how all these changes are also generating challenges to the constitutional rights and privileges we associate with the US Constitution. This review will unfortunately ignore many of the developing conflicts between and within the states, some of which have their own notions about what rights the people should enjoy. Finally, a brief acknowledgement of the contributions being made by politically active groups within the public sphere, like the ACLU, the Electronic Frontier Foundation, and the Leadership Conference on Civil and Human Rights will be made before I turn to some radical ideas about how public opinion could actually play a role in determining what "reasonable expectations of privacy" might actually be.

Identification and beyond

Over time, I have come to talk 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 like 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 (Gandy, 2012). 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, weight, etc.

I often draw a distinction here between identity and identification with the suggestion that 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 (Gandy, 2000). Identification is almost entirely the product of the influence and determination of others, although the individual so identified may have participated in that process by answering a question or checking a box. Although the terms used in identification at this level may be the result of a classificatory exercise, there is a particularly useful value in treating classification as a distinct part of the process because of its association with investigation and discovery, often achieved with the aid of theory, experimentation, and statistical analysis.

In moving beyond classification, identification takes on 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 is an evaluative assessment, or an estimation of the positive or negative outcomes likely to be associated with a particular set of responses. Increasingly actuarial assessments of these outcomes are often compared in terms of risks to be minimized or avoided. What is currently treated as the final stage of this process of identification, is the set of recommendations that should be followed in order to increase the probability that the more desirable responses of the target, or target group members will dominate the outcomes of some interaction.

Identification

Although the identification of individuals in a variety of contexts is often discussed in relation to concerns about privacy (Nissenbaum, 2010), it has been suggested that this interest might also be considered in terms of a right to anonymity. As Slobogin (2002, p.238) reminds us, to be anonymous, is to be nameless. And the value of this state is derived from the limitations on an observer's ability to associate a name with a location or an activity that might influence the characterization and evaluation of the person so identified. Blount (2017, pp. 12-13) explores this aspect of location in terms of the "spatialization of privacy," in which the possibility of having a reasonable expectation of privacy within a variety of public places on the basis of the routine, or usual purposes of the activities in those spaces for which surveillance might otherwise be justified. However, the use of the information gathered for quite different and unrelated purposes would require an explicit warrant with its own justification and notice to the target of that search.

The development of facial recognition technology is just one of many elements of increased capability and use of biometric systems being applied to the identification of individuals (Goldenfein, 2018; Maurer, 2017). These components of the Next Generation Identification system add to the ability of law enforcement agencies to make use of the Interstate Photo System

to “search a database of about 30 million photos to support criminal investigations” (Maurer, 2017, p. 2). The US Government Accountability Office (GAO) has reported that that the Department of Justice (DOJ) has failed to update the Privacy Impact Assessments required by the E-Government Act of 2002 as these systems have continued to be transformed and deployed (Maurer, 2017, pp. 6-7).

A recent GAO report (Maurer, 2017, p. 14) cited comments by the Electronic Frontier Foundation (Lynch, 2017) about error rates in these identification systems suggesting that “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.” Part of the concern expressed by the GAO is based on the fact that the FBI has not made the investments necessary to ensure the accuracy of these systems, especially with regard to the fact that these identifications are being provided by external partners, as well as the possibility that “images of innocent people are unnecessarily included as investigative leads” (Maurer, 2017, p. 18).

Lynch’s extensive testimony (2017) before a House Committee’s hearings on the use of facial recognition technology (FRT) also noted that the burdens imposed by the maldistribution of errors made by these systems will “disproportionately impact people of color” (p. 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” (pp. 17-18). As a result, members of these communities will bear the burdens of the greater proportion of inaccuracies or errors these systems have been demonstrated to make. She also notes that the failure of the FBI to evaluate the discriminatory impact of the Interstate Photo System has been explained as a function of the fact that the system does not actually identify a particular individual as the target, but only provides a “ranked list of candidates,” for which they 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.” The FBI argues that this list is only “an investigative lead not an identification,” and as a result, there would be no “false positive rate” (p. 10). However, the fact that many police departments proceed as though the results of “matches” accomplished with altered and proxy images are sufficient as identifications, despite unreported, but highly variant rankings of candidate targets leads to mounting opposition to the use of these systems (Garvie, 2019)

Classification

The identification of individuals extends in several directions beyond the association of a specific individual with a place and time of birth, and a variety of tokens that associate that individual with a name and with documents bearing that name and other spatial and temporal identifiers that serve to reinforce the confidence of those seeking a unique one of many who share some, but not many such markers of identity.

Our concerns with identification do not end with identity but expand with other associations that facilitate the association of an individual with a particular classification, or characterization of interest to a particular seeker (Steinbock, 2004). Margaret Hu (2017, pp. 651-654) emphasizes the historical, and continual importance of racial and ethnic classification, beginning with the creation of legal and regulatory constraints on the freedom of African Americans that continued

to be enforced, even after the passage of the Thirteenth, Fourteenth and Fifteen Amendments. She suggests that the classification of identity "is an essential step in establishing exclusionary systems" (p. 654), but 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, pp. 655-656).

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" (p. 13). He emphasized the use of searchable databases as an aspect 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 increase role in assessments of risk" (Lyon, 2003, pp.15-16).

Surveillance technology

Advances in the capability of information and communication technologies (ICTs) to gather, process, store and exchange information are transforming the nature of societies around the globe. Much of the attention being paid to the changes being wrought by developments in ICTs is focused on their economic impact at the levels of production, distribution, and marketing. Periodically, the focus on their societal impact is directed toward the social and cultural realm, primarily with regard to entertainment, as well as news and information goods and services. Changes in the nature of interpersonal communication has come to central stage with developments in the nature and influence of social media, and the dominant platforms operating at a global level (Cohen, 2017a). A large part of the concern about the societal impact of social media has centered on its development as an instrument of surveillance and a threat to individual and group privacy, and the levels of autonomy it had traditionally served to protect.

The rate of change in the capabilities of surveillance technology is a major source of the difficulty we face in developing the legal, judicial and regulatory policies needed to ensure that the public interest and social values that we associate with democratic governance continue to be available. The fact that the success of corporations in the age of big data analytics is tied to their ability to convince public and private actors that their success, and perhaps even their survival depends upon their ability to identify, characterize and evaluate the individuals with whom they will interact, we can expect that they 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).

An additional concern is based upon the ease with which images or other templates used to identify and characterize individuals are easily shared across networks with third parties including corporate entities as well as a broad range of departments and agencies within the CJS. This widespread tendency essentially destroys the meaning of informed choice through which individuals submit or cooperate in the use of biometric technology under the assumption that the use of this information is limited to the specific purposes for which it has initially been gathered.

Cameras, fixed and mobile

Although we are focusing our attention primarily on the use of cameras by law enforcement agencies, we are reminded that visual imagery has been used for centuries as 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 (Goldenfein, 2018). Goldenfein (2018) takes us back to Sir Francis Galton's efforts to make use of criminal portraits as aids to discovering the appearance of criminality in order to call our attention to the same kinds of claims being made for the kinds of experimental work being performed today "using new photographic techniques, statistical methodologies, and biological theories." However, Goldenfein (2018, p. 7) notes a shift in the paradigm "from qualitative visual searches for similarity amongst groups toward purely quantitative statistical analysis." In extending the impact of technological advances in imaging, he cites Andrejevic's characterization of neuromarketing as suggesting that the body is more informative about people's tastes and preferences than what they actually say, now that neuroimaging provides almost direct access to the brain (Goldenfein, 2018, p. 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 and Taniguchi et al., 2009).When combined with facial recognition technology, automated CCTV systems are likely to invite law enforcement, or other official responses to the presence of individuals whose images are already in miscreant databases, where there is likely to be an over-representation of the poor and minority members of the nearby community (Slobogin, 2002, p. 249).

Police departments in the US were encouraged to acquire and use body-worn-cameras (BWCs) in response to public protests against police shootings, as well as a resource that would protect police against false claims of abuse of power. President Obama provided substantial support for the acquisition of these cameras and the associated expenses of their use as part of his FY2016 budget (Mateescu, Rosenblat and boyd, 2015). In some jurisdictions, however, local governments have rejected these grants on the basis of concerns about the threats to privacy that they represent (Schmidt, 2019).

As the number of police agencies around the world that have adopted this technology increases, so have the concerns about their impact on the police that wear them, as well as on the members of communities most likely to be archived within their digitized evidence management systems (Palmer, 2016).

Because control over the use of the cameras and the records they generate tends to be under the control of the officers wearing them and the agencies establishing and implementing policies about access and use of the data, a host of questions about access to and use of that data by persons who have been recorded, as well as by other members of the Criminal Justice System (CJC) are increasingly be asked (Beutin, 2017; Mateescu, Rosenblat and boyd, 2015).

Additional concerns are expected to emerge as BWCs capture and distribute continuous live-streamed audiovisual information (Blount, 2017) that is likely to be enhanced with biometric assessments of the identity and emotional state of the individuals, many of whom will not be interacting in any way with a police officer.

With support from federal grants, law enforcement agencies have also acquired car mounted license plate readers. Early adopters of the readers include sheriff's departments in border states. Other applications, not specifically linked to law enforcement, include the use of such cameras to identify and charge users of increasingly automated bridge and highway toll collection facilities. Like other camera-based systems, these devices often have collection, storage, and analytical resources that capture date, time, and location of the vehicle, and on demand, facilitate the development of profiles of the vehicles including the characteristics of the locations and the activities most likely engaged in by the drivers or passengers.

Critical observers suggest that these plate readers are just one among many elements of continuous surveillance systems operated in partnership with commercial firms, that generate massive amounts of data that machine learning and other forms of artificial intelligence translate into strategic information. Law enforcement officials, on the other hand, argue that the collection of this information takes place in public, where there is no reasonable expectation of privacy, and in addition, as some suggest, the mounting of a readable license plate is a government requirement, but unlike the driver's license, which may be requested by the police, it is nearly always on public display (Brayne, 2017).

Biometric identification

The assignment of meaning to or evaluative assessments of the characteristics of the environments, sites, or locations, as well as the dates and times at which the data have been gathered is the specialized value that computational analysis adds to the so-called raw material being collected (Cohen, 2017, 157-161; Couldry and Mejias, 2019).The addition of facial recognition technology to body worn cameras, or to the image processing technology made available to law enforcement as valuable ancillary service, is an especially transformative, or "disruptive" enhancement identified as part of the "violence of algorithms" (Owen, 2015) enabled through "dataveillance" (Cheney-Lippold, 2017).

Facial Recognition

Facial Recognition Technology (FRT) is a rather distinct form of biometric identification in that it 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. This kind of "ground truth" for fingerprints and iris scans generally require cooperation, or at the very least, awareness on the part of the subject of identification, whereas FRT data can be captured and validated from afar, and often without the awareness and cooperation of the target (Nakar and Greenbaum, 2017).

At the same time, the fact that identification and comprehensive classifications of individuals, many of whom do not have criminal records, represents such a significant threat to privacy and

anonymity leads many critical observers to suggest that police should be required to demonstrate a special need to gather this much information (Nakar and Greenbaum, 2017, p. 98).

There are already signs from the California Court of appeals suggesting that the accuracy or precision of the match between a captured image and one or more of some individuals' images scanned within driver's license databases, is largely irrelevant, as the matter of primary concern is whether the investigation that follows the identification results in a conviction (Nakar and Greenbaum, 2017 p. 106, citing *Johnson*, 43 Cal. Rptr. 3d at 597-98).

In addition, the FBI's development of a Next Generation Identification-Interstate Photo System with a database of 30 million images (Maurer, 2017) for use within the agency, and for special uses in support of identification requests from other law enforcement agencies, contributes to increasingly expressed concerns about spreading reliance on the technology. At the same time, the rapidly increasing use of FRT in support of marketing and sales efforts, as well as social and entertainment media applications seems likely to lead to the technology achieving the status of being so widely available, that reasonable expectations of privacy will soon be eliminated as a constraint on their use (Nakar and Greenbaum, 2017).

Affective assessment

While facial recognition is being improved as a feature of surveillance cameras, development of behavioral pattern recognition is promised as a back-up for those cases in which facial images are not of sufficient quality for identification with high confidence. Evidence suggests that reliable identification of individuals on the basis of the analysis of captured images, social media commentary, and audio-visual recordings of interactions with police officers on street corners or automobile stops is bound to improve (Goldenfein, 2018). Additional classificatory aids can be expected to become available following improvements in "automated emotion recognition and classification" (Coudert, Butin, and Métayer, 2015, pp. 759-760), including that being developed from the analysis of images people share through social media platforms, such as Instagram (Reese and Danforth, 2017).

The extent to which already developed and emergent analytics can reliably infer affect and emotion through "automated face analysis" or other facial coding strategies utilizing neural networks, is complicated by the fact that the accuracy of these systems varies with the particular emotional category being displayed (Burr and Cristianini, 2019, p. 11).

While the world of social media and digital communications has helped to create a willingness, if not an highly valued opportunity to express oneself, the use of graphic emoji of varying levels of distinction represents a technologically enabled resource for conveying one's mood to others with the simple press of a button (Davies, 2017). To the extent that the button press represents some degree of willingness to convey some indication of one's affective state, it seems reasonable to distinguish between that process and the capture of additional, or alternative assessments of one's mood by means of behavioral analysis. Arguably, this analytical step can be considered an example of an ungranted taking of something of value (Davies, 2017, p. 35). As the technology for the capture of this information for the purpose of control or at least influence over the subject of assessment increases in scope and power, it becomes yet another means by

which “bodies become objectified as natural entities or capital” (Davies, 2017, p. 39), by which data captured from the many become resources for the few (Whittaker and Crawford, et al., 2018).

Remote sensing and statistical surveillance

While remote sensing is generally associated with photographic or other imaging technologies capable of producing identifiable representations of targets of interest, in an era in which big data analysis is providing inferential assessments of members of smaller and smaller groups of individuals, statistical surveillance is also being recognized as remote sensing (Gandy, 2012).

Statistical surveillance provides “actionable intelligence” about members of “groups” that are likely to have no legal status of the sort afforded to members of other groups that have been granted constitutional protections, in part as compensation for the burdens of discrimination that they have experienced in the past. Indeed, because the identification of the groups to which these individuals are said to belong is usually a matter of tightly held corporate or agency secrecy, most of us have no knowledge of the groups to which we have been assigned. In part, it is because the protections of the law in the US are focused almost entirely upon identifiable individuals, rather than on members of idiosyncratically defined groups, the challenges represented by the expansion of statistical surveillance have continued to expand while the ability of the law to respond continues to fall behind.

Computation and Big Data

Margaret Hu (2017) offers us an introduction 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” (p. 639). As we will discuss, these emergent systems are being used for the identification and classification of individuals and groups, as well as the places in which they make their homes, in order to predict how these targets of interest will respond to opportunities and threats, which have been designed to be both efficient and effective in achieving the outcomes that discriminatory system users prefer.

The strategic use of data for the identification and classification of persons, places and things is not new (Bowker and Star, 1999). What is new is the ability of computational systems to locate, gather and analyze such massive amounts of data and put it to use in a variety of ways that had only been imagined by the authors of science fiction novels in the past. A particularly important part of this development is the extent to which the data that are being used are not being gathered from highly structured files or databases that have been organized by researchers and analysts to serve a particular purpose, but are being derived from a variety of environmental sensors that have been taught, and increasingly have learned on their own how to make sense of the patterns they encounter within the world (Atzori and Iera, et al., 2010).

A related concern is the nature of the variance in the accuracy and reliability of the products of these analyses as they are used to affect the life chances of members of different population segments. As Barocas and Selbst (2016) remind us, there are a variety of decisions that are made

in the collection and processing of available data that lead to the denial of opportunity, and the imposition of constraints upon members of "protected classes" that reproduce and reinforce adverse impacts that add to the disproportionate burdens they already bear. Many of these disparate impacts are derived from the fact that the samples from which data are drawn are not representative of the populations about which these concerns are most relevant. And while under-representation is the most common source of bias in the data, they note that over-representation can also result in the maldistribution of opportunity based on unequal attention being paid to members of a group that has been assigned a rating associated with a negative stereotype (Barocas and Selbst, 2016, pp. 686-687).

An additional concern, one that is especially important with 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 actually have vitally important public policy implications that are increasingly being treated primarily as engineering or design problems. Miller (2014 p. 124) invites us to consider that an early decision about setting initial tolerances for performance in prediction usually involves setting different value levels for positive and negative errors, which are actually critically important policy decisions that need to be taken at public, and then administrative agency levels.

Analytics and data science

We are just coming to appreciate the changing nature of the paths being taken through analytics from facts, or the indicators of truth about the world into recorded data that can be turned into information that facilitates understanding, and perhaps even knowledge and wisdom (Hayes, 1993). While we are far less appreciative of that part of the path that increasingly ignores the benefits of understanding and wisdom, settling instead for more accurate and reliable predictions, we do understand some of the motivations guiding some of those who have chosen a particular path (Brayne, 2017, p. 980).

Nevertheless, we hold out hope that a commitment to providing explanations for the patterns that we observe in the world so that we can change them (Frameworks Institute, 2019) will not be diminished. In particular, as we will explore below, it is vitally important to understand how and why an actuarial focus on the estimation and evaluation of risk within different levels and stages of public interactions within the CJS (Weisburd and Majmundar, 2017) is limiting the role of developed theory and experience in shaping the futures of those caught up in an expanding surveillance web.

Movement along this path toward increased emphasis on predictive assessments within the CJS is being influenced greatly by significant enhancement of the capabilities of digital computing systems to acquire and process data without constant operational management by humans. Machine learning (ML) has been identified as an aspect of artificial intelligence (AI) with particular relevance for the exploitation of big, or massive data in countless applications from search engines and medical diagnoses to facial recognition and automated weapons (Berman, 2018, pp. 1278-79). While machine learning can be thought of as an especially powerful resource for data mining, the algorithms it relies upon to identify meaningful, and perhaps unimagined patterns within a particular dataset, are somewhat special in that they "are able to

learn from experience and become more accurate over time" (Berman, 2018, p. 1279). It is this enhanced capability to learn from experience, rather than from the training of system developers that leads to the expectation that AI/ML technologies will soon outperform humans in a great variety of tasks or industries, including those of policing and law enforcement, that are vitally important within the global economy (Bollier, 2018).

Of particular interest in these developments is the fact that the analytical processes used by computational classifiers are not necessarily recognizable variants of the cues or data elements used by human classifiers. For example, a recent evaluation of computational analyses of individually posted Instagram images were used by researchers to evaluate the accuracy of their machine learning generated predictions about whether or not the posters were or would soon become diagnosed as depressed. Researchers noted that the correlations between features used by the computer, and those used by human coders to make these predictions were "extremely low," while the correlations between human raters "showed strong patterns of correlation with one another" (Reese and Danforth, 2017, p. 8). Arguably, this is an aspect of the difficulties we are likely to face as we seek to understand how algorithmic assessments, predictions, and recommendations are being made and then put to use (Knight, 2017; Sackler and Sackler, 2017; Selbst, et al, 2019).

Accuracy, Bias, and Fairness

Brauneis and Goodman (2018) also suggest that the values that guide decisions made by commercial vendors, and the engineers who develop their systems are not likely to share the values and concerns that are more common within governments, and among large segments of the public. Considerations of fairness are not only far less likely to be among the concerns demanding the attention of engineers, ensuring fairness is also among the more challenging requirements that are now being placed on algorithmic systems (Selbst, et al., 2019). Even though there are efforts among designers of machine learning systems to "engineer fairer and more just machine learning algorithms and models by using fairness itself as a property of the (black box) systems… They consider the machine learning model, the inputs, and the outputs, and abstract away any context that surrounds this system" (Selbst, et al., 2019, p. 2). Unfortunately, context is a critical determinant of the meaning of fairness as it varies across the sociotechnical terrains in which algorithmic decision making is becoming the norm.

And while AI/ML systems are assumed to be capable of processing massive amounts of data, we cannot forget that by their nature "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, p. 123). A further complication, of course, is the fact that these groups may actually be the product of some algorithmic classificatory process, rather than a development produced by a collaborative or legal process that may have assigned particular rights and privileges to the members of those groups.

The choice of the groups, for whom the achievement of a particular form of algorithmic fairness is not only meaningful, but highly valued, places the members of the community of "fair-ML practitioners and researchers" in the position of altering the distribution of a unique collection of benefits (Selbst, et al., 2018, p. 11). The fact that the members of these groups may be ignorant

of their membership status and the benefits or burdens that are associated with it complicates the challenges involved in organizing such an effort under the guidance of a participatory democratic process (Gandy, 2006, 2009). In addition, there are expressions of doubt and concern that the paths being chosen for the articulation and pursuit of fair AI/ML standards and strategies of enforcement will not be able to overcome the constraints that a "business ethics" orientation, rather than one emphasizing social justice places on the corporate commitment to ethical design (Greene and Hoffman, et al., 2019). The impact of this particular orientation is reflected in the fact that 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 and Hoffman, et al., 2019, p. 2127). Those are the kinds of decisions that should be explored and decided within the democratic process, rather than one limited to experts and technicians.

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, but it is also important to take note of the fact that commercial providers of surveillance-oriented services count government agencies, including the police, among their most reliable and profitable customers. As Miller (2014, p. 120) suggests, predictive technologies, initially designed and marketed to law enforcement agencies, find application in secondary markets, where budget constrained government agencies are prime candidates for their own versions of systems designed to identify members of their client populations or networks for whom a bit more attention will generate meaningful benefits to their bottom lines, or measures of performance.

A special concern arises when the corporate providers of what appears to have become essential technology for law enforcement agencies are also the dominant firms in that market, enjoying an almost pure monopoly. As a result, the opportunities for even large city police departments to negotiate the conditions of sale, rental, or critical services, suggests that they often do so at a disadvantage as contract takers rather than negotiators. This special relationship is due to the fact that it is not so much the fixed and mobile cameras, but the specialized cloud-based data management services that are far more expensive, and also require long-term high value contracts (Gelles, 2016; Joh, 2017, p. 114).

As Joh (2017, p.120) notes, the special relationships that are imposed upon the police agencies as contract takers often leaves agency officials without a detailed understanding about the extent to which they actually own, and thereby control the use of the data that their surveillance systems generate. The result of this uncertainty means that these private companies are able to "exert an undue influence" that can "affect legal change, police oversight, and police accountability."

A dominant actor within the BWC market is Axon, previously known as Taser International, primarily for its popular stun guns. Axon is rapidly establishing leadership in the marketing of BWCs. Axon 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). Concerns about the uses to which Axon will put the data that it manages for police departments, are also beginning to be expressed. For example, it is reported that Axon

will use the massive amounts of video it stores for its clients to train its AI systems to reduce the time and effort that police officers, and perhaps even prosecutors and judges would have to spend to make efficient and effective use of that data for many of their routine tasks, such as characterizing interactions with the public and drafting initial reports (Greene and Patterson, 2018). The early signs of their efforts to develop these applications, including those thought to include facial recognition, do not invite much confidence about their ability or commitment to avoid the kinds of errors that are raising concerns among data scientists (Zhang and Neill, 2017).

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 includes a multidimensional network of judicial personnel, including those working at different levels of a system of courts, and yet another network of specialists that manage the penal system. These agencies operate within jurisdictions from cities through counties, states and federal levels. 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 with these objects of interest is continually being transformed by changes in the ICTs they have come to rely on (Gandy, 2009, pp. 123-143).

Police

A fundamental shift has taken place in the nature of policing to a "more proactive, predictive and... pre-emptive policing" that is marked by "increased reliance on surveillance technology" (van Brakel and De Hert, 2011-13, p. 165). This technology involves a form of profiling, generally understood as the assignment of individuals to "groups" on the basis of shared attributes, including behaviors associated with, or predicted on the basis of correlations generated algorithmically through the processing of data not specifically associated with criminal activity. Indeed, concerns that are being expressed with regard to the collection and use of personal data from individuals who have not been charged with a crime, or in many cases, not even been the subject of a targeted investigation by a law enforcement agency that are being justified on the basis of an expectation that this kind of information and analysis can be used to prevent crimes in the future by focusing attention upon people who have an algorithmically assigned rating of meaningful risk (van Brakel and De Hert, 2011-13, pp. 182-183).

There are also concerns about the extent of control that officers have over their cameras, especially with regard to whether they should determine when to turn the cameras on and off (Fussell, 2018). In response to these concerns, some BWCs were offered with a cache memory feature that allowed the device to retain the footage that had been captured before an officer actually turned on the camera when an event, or interaction began. Circumstances that were captured during the brief periods before recording was initiated by the officer could prove to be influential in characterizing and evaluating what happened after the camera was turned on (Hung, Babin and Coberly, 2016).

A critical issue arising from officer control over when recording begins and ends, as well as when officers, other members of the CJS, including prosecutors can review the captured footage, is the extent to which the review alters the memory of the officers involved in an interaction with the public. Policies with regard to officers viewing recordings prior to writing their official reports are especially important in this regard (Hung, Babin and Coberly, 2016, pp. 6-34 to 6-35).

Despite some of the earlier expressions of hope that the widespread use of BWCs would increase the transparency and accountability of police agencies and their officers, mounting evidence and argumentation suggests that the police have been the greatest beneficiaries of the spread of this technology. Among the benefits to the police as front-line agencies within the CJS, the widespread use of BWCs is said to have resulted in fewer complaints against the police. No doubt some of that decline can be attributed to reductions in the use of force by police against members of the public, especially those from racial and ethnic minority groups. The fact that there has been a reduction in the number of offenses against officers by members of those groups, suggests that awareness of the recording of such interactions tempers the behavior of both the public and the police (Palmer, 2016).

Prosecutors and judges

Prosecutors have a strategic advantage over defense attorneys in their access to the material captured by BWCs. They "simply treat the videos as another type of discovery, another relevant piece of evidence that they do not have to disclose until well after first appearance, arraignment, bail argument, and even guilty plea" (Sacharoff and Lustbader, 2017, p. 274). An additional disadvantage for defense attorneys and their clients is the fact that they are routinely denied access to the kind of information that would guide them in accepting or seeking to negotiate the details of a plea agreement. This is especially important given the fact that "approximately 94% of state cases plead out" (Sacharoff and Lustbader, 2017, p. 276).

Concerns about the use of decision assistance technology by judges and prosecutors are based in the belief that there is a potential for them to amplify and naturalize longstanding biases, all the while making them more difficult to recognize, understand and correct (Burrell, 2016; Campolo and Sanfilippo, et al., 2017, p. 4). A somewhat more challenging tasks for judges arises when they are expected to stand in for or make assumptions about what the average person feels is reasonable with regard to their expectations of privacy. The evidence is quite strong in its suggestion that the opinions of judges about the reasonableness of efforts by police, are distorted by a tendency to give algorithmic systems the benefit of the doubt.

Reliance on "decision-assistance systems," such as those which recommend sentences, bail, probation, drug testing, or other activities designed to manage the environmental influences believed to encourage misbehavior by an individual at a particular stage in the process of rehabilitation, is not designed to replace human managers within the CJS, but to assist them in choosing the appropriate opportunities and constraints that are most appropriate for a particular individual. However, the fact that these systems are not actually designed for predictions that apply to a particular individual, but for a population segment that shares a similar pattern of

lifetime experiences, especially those involving the CJS, heightens the challenges involved in evaluating their performance (Bollier, 2018).

Challenges to traditional policing

The term that is increasingly used as a description of the efforts by police agencies to prevent or reduce crime is "proactive policing." 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, p. S-1).

Among several approaches to proactive policing, the one identified as a "place-based approach" incorporates a number of elements that rely upon technologically-based strategies and resources that are based on evidence "for the concentration of crime at micro-geographic places." Those places then become targets for "predictive policing," "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 Majmundar, 2017, p. S-2). What they all have in common is their increased reliance upon data gathering and analysis that 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, as well as the constitutional protections that limit their ability to use strategies that may "raise concerns about deeper legal values such as privacy, equality, autonomy, accountability, and transparency" (Weisburd and Majmundar, 2017, p. S-4).

At the same time, there are signs that critical engagement with the transformations in policing that are associated with big data analytics have helped to focus attention on the possibility that the analytical lens of data-based surveillance might be focused on the behavior of police in ways that might identify patterns of unconstitutional acts. An important part of such a development, despite the kinds of active resistance that such a shift in attention will stimulate, is a shift from the traditional focus on the "one bad apple," within a department, toward an emphasis on systematic patterns of behavior indicative of "systemic racial bias" (Ferguson, 2019, p. 561). Unfortunately, the assumptions and claims that have been made about the scope of big data as being all-inclusive, don't actually apply to readily accessible data about the behavior of police, in part because these departments tend not to keep those sorts of records. The kinds of analysis that are most common in the recent past and the likely future are the investigations of particular departments by the US Department of Justice Civil Rights Division (Ferguson, 2019, p. 587).

Predictive policing

Predictive policing has been said to be the "holy grail of policing—stopping crime before it happens" (Ferguson, 2017, p. 1117). Evidence suggests that we are clearly 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: 1) the predictions of the places and times in which particular types of crimes are more likely to occur; 2) the prediction and identification of those individuals who are most likely to commit those crimes; and 3) the identification of individuals who are most likely to become the victims of crime (Degeling and Berendt, 2018). Other applications by police departments include social network analysis that generates a variety of maps that "link friends, gangs, and enemies in a visual web of potential criminal actors" that might be approached in time to prevent some of the violent interactions that are common within these networks (Ferguson, 2017, p. 1118). Arguably, these applications of predictive algorithms do 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).

Questions about the sources of the data that have been relied upon for the development and testing of the algorithms and the evaluation of the nature and extent of the errors that vary across geodemographic population segments are of particular importance when these predictions are used to guide the allocation of scarce resources by police departments.

Reasonable suspicion

Miller (2014, p. 126-128) provides an overview of the increasingly meaningless protections of privacy derived from decisions by courts at the appellate level that reduce the weight of the requirements for "probable cause" in order to justify the grant of a warrant for searching persons, documents and homes. What was initially a fairly meaningful standard has been, over time, relaxed for particular kinds of searches, meaning that officers only needed to have a "reasonable suspicion" that an individual was criminally active. A more substantial reduction in the coverage of a privacy right came with the specification of the standard of "relevance to an investigation,' in order for a subpoena to be issued. And perhaps, the most consequential damage to the protections once associated with the Fourth Amendment came with the developments in "third-party doctrine," which meant that a "reasonable expectation of privacy" would no longer apply to most digital interactions, and not even a claim of relevance would be required for most of the searches of transaction data. Once again, consideration of the nature and extent of false positives that are likely to be generated by automated surveillance of millions of innocent persons will be necessary for a determination by the courts (or the legislatures), that the burdens being imposed on the public are not justified by the accumulated benefits of reductions in different kinds of crime.

The decline of protections against invasions of privacy that are associated with the rise in mass surveillance is also linked to the increased use of facial recognition technology. Critical responses to the use of facial recognition by law enforcement agencies emphasize the absence of reasonable suspicion as a justification for the kinds of searches that become routine 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. Merely having a driver's license in the majority of states in the US puts thousands of innocents at risk of mis-identification, followed by a stressful, if not actually dangerous interaction with a police officer (Bedoya, 2017). The fact that the facial recognition systems presently in use have

substantial error rates, and that the number of innocent persons placed at risk by these errors increases with the size and nature of the databases used in those searches, becomes even more troubling when we add in the fact that erroneous identifications are more likely to be made in searches for African Americans, women, and members of other non-white racial or ethnic groups (Bedoya, 2017, pp. 12-13).

An important source of concern for police are the consequences that are likely to flow from greater reliance upon information and strategic recommendations derived from a variety of automated, and semi-automated devices and systems. Among the complications arising from police reliance upon algorithms, rather than confidential informants, is that individual officers will become increasingly unable to provide their own reasons for deciding to stop and search a particular pedestrian, or a motorist whose license plate triggered a recommendation to stop a particular vehicle (Berman, 2018, p. 1350).

As the police rely more on algorithmically-derived guidance about whom to stop, question and search, 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, 2016a; Goel, et al., 2017; Mateescu and Rosenblat et al., 2015; Miller, 2014). Thus, 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 (Joh, 2017, p. 125).

Evidence management

While there are a variety of concerns associated with the maintenance of evidence within police custody, there are even more concerns being raised "in 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, p. 42). Concerns related to police management of evidence come primarily from two directions: one associated with limited resources, knowledge and capabilities, the other associated with self-interest, where law enforcement personnel may attempt to modify records to achieve goals or avoid critical sanctions.

Both accidental and intentional decisions have resulted in declines in the status of evidentiary records, critical in determining the outcome of a trial or criminal proceeding. "These 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, p. 45) from Axon or one of their competitors. Some of those complications have to do with the determination of data ownership rights, as Axon is arguably is 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 these data. As Wood (2017, p. 47) sees it, entering "into the contract in the first place implies that the cost and expertise of building and managing large-scale technological infrastructure lie outside of the capabilities of law-enforcement agencies." Negotiations over the determination of the status of law-enforcement camera data as public records continue to challenge courts, states, and municipal governments.

It should be noted, however, that those who make public policy regarding the use of BWCs are not focused primarily on the usefulness of this technology for collection of evidence; a substantial interest has been demonstrated to be focused on the use of the cameras to support both the transparency and the accountability of with regard to their interactions with the public at large (Wenner, 2016, pp. 900-906).

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. Transparency and accountability depend fundamentally 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 across throughout the population (Ananny and Crawford, 2016). Unfortunately, especially with regard to information about the use of technology by the police, there are a variety of barriers to accessing relevant information that limits the possibility of success (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 that include the storage and processing of the transaction-generated information (TGI) that limit disclosure of details about the underlying operational systems, their development, testing, and performance.

There are also limitations based in the need for specialized knowledge to understand how the algorithmic systems generate the identifications, classifications, evaluations, predictions and strategies for stopping crime before it happens (Knight, 2017). 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, pp. 6-12). The broad exceptions to rules that would limit the ability of individuals to oppose automated decisions are primarily enacted with regard to “law enforcement and national security-related data processing” (Rieke, et al., 2018, p. 26). This is part of the challenge we face in somehow separating 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, p. 6). As Cohen (2017b, p. 12) 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.”

Additional problems arise with regard to applicable standards that apply when liability or the responsibility for harm has to be assigned to a single individual or to a leader of a corporation or government agency (Selbst, 2019; Wood, 2017), when in fact, the algorithmic systems that are making, or shaping life altering decisions are actually a complex assemblage, a continually changing actor-network (Ananny and Crawford, 2016 p. 11).

An important insight into the variety of concerns that are associated with the increased role of automated technologies is the fact that governmental agencies, especially those responsible for

the management of the CJS, are constrained by their budgets, and as a result are relying on 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 (Knight, 2017), "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, p. 109).

Part of the problem we face with regard to accountability 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, and the software and applications engineers that design the systems (Binns, 2018), as well as 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, p. 22). As Binns (2018, p. 548) suggests, however, 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."

As noted earlier, the widespread adoption of 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 general patterns that have developed for the control of the audio and video evidence captured by these cameras, placed them under the control of the police departments, or in a contractually mandated joint operational arrangement with the vendor of the cameras and the evidentiary materials (Sacharoff and Lustbader, 2017; Yu et al., 2017).

Although the initial public support for the acquisition and use of the cameras emphasized their use in support of improving the transparency and accountability of police officers, the evidence to date suggests that the primary use of these resources is in the prosecution of "ordinary criminal cases, including misdemeanors such as resisting arrest and more serious drug offenses." Data suggest that "body camera videos are used far more often against ordinary citizens than the police" (Sacharoff and Lustbader, 2017, pp. 273-4).

President Obama's Task Force on 21st Century Policing is said to reflect a perceived need to ensure that in the face of more video from personal cameras in their telephones used by members of the public that are then distributed widely through social media, the police need to ensure that video from an officer's perspective can also be made available for the public to view. In her view, Beutin (2017, p. 15) suggests that "the report makes it clear that its main endorsements of and reservations with cameras lie in protecting the police" but Obama's construction of their usage was more expansive, in that they were expected to "improve community trust, transparency, and accountability" (Obama, 2017, pp. 864-865).

One of the factors that limit the use of Freedom of Information Act (FOIA) requests as they apply to BWC data is uncertainty about the extent to which the data captured by the cameras, and the assessments arrived at through secondary analysis will necessarily be treated as public records. While there is little support for a categorical exemption for data gathered by police

technology, there are legitimate and influential arguments against disclosure on the basis of privacy concerns (Wenner, 2016).

The existing exemption from the provisions of FOIA depends upon an authoritative claim that the information of interest had been "compiled for law enforcement purposes," and that disclosure of that information would result a well specified set of "harms." Two of those harms are those that are likely to "interfere with enforcement proceedings," or "constitute an unwarranted invasion of personal privacy" (Wenner, 2016, p. 873). The first harm is likely to result from strategic use of FOIA by the targets of the investigation, perhaps to enable the destruction or alteration of evidence. A somewhat more complicated set of requirements applies to the concerns about the invasion of privacy. Not only must there be a basis for claiming that the privacy loss was likely, but it must also be demonstrably "unwarranted," that is, the "costs of the invasion must outweigh the benefits of the disclosure" (Wenner, 2016, p. 882).

The exemptions being sought with regard to BWCs are closely related to limitations on defendants or litigants gaining access to information that would "expose and undermine the extent of the government's investigation." The problem is that BWCs are primarily used in the context of encounters between officers and members of the public, rather than in "investigations of systematic police misconduct." It is interesting to learn that "courts have been particularly favorable to finding a strong public interest in allegations of police misconduct" which would suggest that WBCs can potentially support expectations of transparency and accountability as it applies to police behavior, especially in the context of "the numerous high-profile examples of video evidence contradicting official police accounts of shootings"(Wenner, 2016, p. 600).

The Challenges to constitutional rights

Although the dust has barely settled around the negotiations involved in the development and implementation of the European Union's General Data Protection Regulation (GDPR), it is clear that it represents a dramatic move forward when compared to the status of laws governing personal information or data in the US (Degeling and Utz, et al., 2019; Goldenfein, 2018, pp. 23-25). There is still no expressed right of privacy in the US Constitution or its Amendments (Solove and Rotenberg, 2003, p. 20), although legal scholars find expressions of such a right "in the penumbras of the First, Third, Fourth and Fifth Amendments" as well as "the Fourteenth Amendment's Due Process Clause" (Slobogin, 2002, p. 263).

First Amendment

First Amendment considerations are associated primarily with the use of algorithmic identification technologies, including facial recognition, to identify individuals who are participating in activities involving protest or political speech in public spaces that would not otherwise be protected by reasonable expectations of privacy (Bedoya, 2017; Lynch, 2017). First Amendment considerations also raise privacy concerns for individuals and communities whose information is captured and stored in public records, including those created through the storage of audio-visual records of encounters with police and other government agencies (Kampfe, 2015, pp. 1169-1175; Metcalf and Crawford, 2016); Solove and Rotenberg, 2003, pp. 566-670).

The right to anonymity is said to be a central value protected by the First Amendment, readily identified with the right to engage in anonymous free speech, association and movement. However, like privacy, there is apparently no explicit constitutional right to anonymity, such that its application with regard to non-political speech is not at all assured, and there are many examples of legislative and judicial limits on the wearing of masks in public (Nakar and Greenbaum, 2017, pp. 117-118).

Fourth Amendment

The Fourth and Fifth Amendments of the US Constitution are identified as providing the most extensive limits on the government's ability to gather information about individuals. The Fourth is the most extensive in its coverage of the limits on government framed in terms of the right to be secure against "unreasonable searches and seizures," and individuals only face the imposition of search warrants upon probable cause and specification regarding the nature of things to be seized. The Fifth declares that no one shall be compelled in a criminal case to be a "witness against himself." This is understood as establishing a "privilege against self-incrimination" (Solove and Rotenberg, 2003, p. 276).

In the face of rather dramatic changes in the nature of information technology and the access to information about direct and indirect paths to information about individuals, there are increasing doubts about the extent to which these Amendments are able to reliably define either unreasonable search and seizure or self-incrimination.

The difficulties in realizing the protections of the Fourth Amendment, especially in public, and more specifically related to BWCs, is the determination by courts that visual images captured by cameras do not "meaningfully interfere" with anything an individual actually possesses. Camera images are produced with reflections of light, for which individuals have no articulable property interests. The Supreme Court has actually ruled that "law enforcement officers may generally record footage that they can lawfully see and hear without violating the Fourth Amendment" (Hung, Babin and Coberly, 2016, p. 7:39).

The rules become a bit more complicated with regard to the audio portions of the interactions between police and members of the public with whom they are interacting. Interpretations of the Federal Electronic Communications Privacy Act actually include oral communication, and not all jurisdictions permit recording of conversations if only one participant grants consent, which suggests that the audio portion of BWC recordings may be illegal (Hung, Babin and Coberly, 2016, p. 7:40). Additional problems along these lines arise when police enter a private residence in response to a report of a domestic violence event in process, or during any other occasions when officers are granted entry to gather information.

It is important to understand how the reasonableness standard as it applies to the protection of rights under the Fourth Amendment should, but has not been subjected to verification in terms of what actually are the "reasonable expectations of ordinary members of the public" with regard to surveillance by police and its threats to privacy, liberty and autonomy (Chao and Durso, et al., 2018).

As Blount (2017) and others suggest, the rapid, and largely automated association of an image captured by an officer, or a device mounted on a vehicle, building, or distant satellite, with a variety of other assessments made in the past, or on-the-spot by sophisticated cloud-based analytics, amounts to a search for which no articulable basis or justification needed to have been arrived at by any human being. This is at the heart of concerns about "the constitutionality of capturing and logging identities without cause" (Blount, 2017, p. 67).

The nature of the records captured by BWCs mark an important shift in the meaning of the kinds of acceptable observations that might take place within a home, including one in which entry has been accomplished with a warrant specifying the focus of that search. Courts have varied in their characterization of "cursory plain-view searches" that would become a "far more invasive and thorough inventory search" if a walk-through had been captured on video which could then be viewed repeatedly, in slow motion, and with enlargement (Zwart, 2018, pp. 800-801).

In the context of predictive policing strategies, extended through the analysis of massive amounts of data where none of the individual bits of information are likely to rise to the level of an invasion of privacy, the amount of information about that individual that can be combined and processed in the aggregate (Metcalf and Crawford, 2016) still raises legitimate Fourth Amendment concerns (Joh, 2016a, p, 60). The standard developed in the Kyllo case, in which the police used thermal imaging to identify the use of grow lamps for marijuana cultivation, was that a reasonable expectation of privacy could be said to exist if the technology was not in general public use (Blount, 2017, p. 71). The kinds of searches and analyses enabled through the use of sophisticated algorithms optimized through the use machine learning or other Artificial Intelligence (AI) are not at all likely to be in general public use (Blount, 2017; Campolo and Sanfilippo, et al., 2017).

There is widespread, if not general agreement among legal scholars that the Fourth Amendment has been rendered incapable of addressing the kinds of racial and ethnic discrimination that are increasingly associated with reliance on the algorithmic assessments that are routinely made by predictive policing technology. This is primarily because while the disparate impacts are statistically obvious, the process that generates them is not easily characterized as racial profiling (Selbst, 2017). There is rarely any evidence of intentional discrimination, based on some disregard for members of a particular racial or ethnic group. This lack of evidence is in part determined by the ability of corporate suppliers of surveillance technology, to insist on their secrecy, which essentially "removes the legal issue from judicial review," as well as likely challenges by criminal defendants (Joh, 2017, p. 120).

Blount (2017), and others (Hung, and Babin et al., 2016) also suggest that the ability of individuals to claim protections of their privacy under the Fourth Amendment is actually weakened in face of development of a "Third Party Doctrine" that raises the level of privacy risk when the information from surveillance cameras and other digital technologies are stored, managed, and processed by third parties as a commercial service, often provided through contract to law enforcement agencies. It is the sharing of that information across agencies, as well as the likely integration of data from different public and private sources that raises questions about the need for warrants for such information sharing. The nature of the policies

pursued by police departments vary according to the nature of the material being stored (whether it is considered evidentiary or non-evidentiary).

Fifth Amendment

Although the Fifth Amendment of the Constitution is not often mentioned with regard to surveillance by the police, references to the importance of due process with regard to the assignment of individuals to categories of interest or concern by the police and other members of the CJS are being seen more often in the context of changes being brought about increased use of big data for predictive analytics.

As Steinbock (2004, p. 752) notes, citing the Court in *Fisher v. United States*, that the Fifth Amendment protects us from being compelled to provide self-incriminating information. However, "the self-incrimination privilege is not available to a customer, patient, or client of a third party [that is required by warrant] to produce its records relating to that person." He suggests that most "if not all, database material would probably come from third parties; if so, no Fifth Amendment self-incrimination rights would be affected." Indeed, it is difficult to overstate the importance of third-party sources, such as the highly personal information that individuals voluntarily share with other people when they are undergoing particular challenges in their lives (Nissenbaum, 2010, p. 226), that makes its way into predictive profiles of potential use to police.

Steinbock (2004), whose oft-cited article is focused primarily on national identity cards, nevertheless does raise important questions about the extent to which demanding a card could be seen as a form of self-incrimination if it enables access to criminal records and other personal information that leads to expanding the nature and length of the stop. He also raises concerns about the use of an identity card (or biometric identification with the use of cameras) to link individuals with "greater numbers of databases, leading to a greater potential impact on privacy and a corresponding diminution of anonymity" (p. 736). "The individual has no way of knowing the contents of the database against which their identification is being run, whether these contents are accurate or not, or what further impositions might be triggered by the information linked to their identity card. This uncertainty will turn every identification demand into cause for apprehension" (Steinbock, 2004, p. 739).

Not only would people forced to go through identity checkpoints experience some degree of fear and surprise, but also knowing that this has become a permanent part of the social fabric would diminish their sense of liberty" (Steinbock, 2004, p. 740). However, consideration of the use of BWCs side-steps the request for identification as the cameras can be expected to provide rapid access to data about an individual on the basis of image processing and identification features of the camera software.

An additional consideration of reasonableness emerges when an individual is recorded, even incidentally, by an officer's BWC. It can be argued that while their faces may be in public, the data and the procedures used to characterize an individual whose image has been captured by a surveillance camera are not localized, and not based primarily on the processing of the facial images just captured. This emergent perspective on the nature of reasonable expectations is referred to as the "Mosiac Theory," in which the point of contention is the use of previously

stored data that transforms the nature of the search that produces insights through aggregation and analysis that no single capture of a facial image useful for identifying a unique individual could provide (Blount, 2017, pp. 73-76). It is also unlikely that the sophisticated analytics being applied to the classification of passers-by on the street or in the park, are yet in common use, and as a result, a reasonable expectation of privacy with regard to their cognitive or affective states should still be arguable before the courts.

Justice Sotomayor's comments in this regard helps to clarify the meaning of reasonableness in relation to what an average person would imagine themselves being subject to. While one could reasonably expect that the police could capture information about an automobile's presence at a particular location at a particular moment in time, few would expect that the police or anyone else could develop a continuous record of the path, stops, and movements of that particular car over an extended period of time (Blount, 2017). The fact that characterization of those various stopping places, and the sorts of people who also stop there, perhaps at the same time as the car of the investigative target, arguably rises to the level of a search requiring authorization because this kind of data-gathering and analysis is likely to reveal both personal and private information.

Due process and discrimination

The fact that discrimination against members of "constitutionally protected classes" is barred in both commercial and government interactions ignores the increasing evidence that members of those groups, and countless others are subject to discrimination on the basis of their having been assigned to a continually expanding variety of groups for which there are no such protections. These population segments are still burdened by disparate-impact consequences of a kind of "Algorithmic Jim Crow" that excludes them from access to goods and services and opportunities because they have been classified as being "unsuitable" (Hu, 2017, p. 694).

However, the limitations on the ability of many of the users, or decision-makers about the use of algorithmic recommending systems, to explain how their systems generate their recommendations, means that it is also difficult for those deciders to justify to justify the use of a technology because of its special ability to meet the needs of the organization. This raises the possibility for disparate impact claims to have force within the law at least as it applies to members of protected classes (Kim, 2017). However, when the decisions are being made on the basis of statistical correlations, rather than causally associated theory, there needs to be a well-articulated justification for using a system that has been demonstrated to produce biased recommendations. Part of the problem here is the fact that most of the users will be constrained by the trade secret contracts they entered with their near monopoly providers of the device and associated processing services. These contracts usually mean that access to the "black box" and the "secret sauce" will not be available to the victims or their representatives.

At the heart of this doctrine is the suggestion that "notice and choice" provides the protections individuals need in order to protect their privacy. However, limitations on notice and choice have been explored in some detail in other privacy-related discussions. The notice part, especially with regard to AI and its inscrutability, even to experts, is rapidly becoming meaningless. The choice part is also becoming worthless, as the social pressures have been amplified dramatically

by the rise in the importance of social media platforms like Facebook. Cohen (2017b, p. 8) describes the extent to which people have come to rely upon the digital information platforms to connect with others as well as to engage in their own "self-presentation." As she (Cohen, 2017a, p. 148) sees it:

> From the perspective of users, advertisers and niche platforms, dominant platforms like Google and Facebook function in a manner analogous to utilities, supplying basic information services now deemed essential to a wide variety of economic and social activities.

Cohen suggests (2017b, p. 8) that these platforms "are designed to encourage and reward practices of self-exposure and peer exposure" to such an extent that choosing whether to engage or not in these systems of networked surveillance is not really a meaningful option. As she sees it, "the ability to control the terms of self-exposure in networked space is largely illusory."

Daniel Citron (2008) provides an oft-cited exploration of the impact of technological changes in the processing of data about individuals that raises concerns about limits on the ability of individuals who may have been harmed as a result of bias or error in the technological systems that are used in their identification, characterization and assessment by government agencies. As she suggests, the continually changing automated systems being used in these agencies is increasingly less accessible to members of the public affected by their determinations, and as a result, the transparency and accountability that procedural justice requires is being denied (p. 1254).

Citron's critical evaluation of the development and use of automated systems takes due note of the tendency among system users to give the benefit of the doubt to the technology, while routinely rejecting claims about system errors made by individuals seeking some accommodation. This "automation bias effectively turns a computer program's suggested answer into a trusted final decision" (Citron, 2008, p. 1272). The problems that we are losing sight of with regard to the impact of automation bias on predictive crime systems are based on the fact that even those "mixed-mode" systems where there is a requirement for review by a human being before a recommendation is implemented are unlikely to challenge the recommendations made by the computer (Miller, 2014, p. 122).

In addition, the fact that few systems generate audit trails makes it difficult, if not impossible for staff to tell a claimant the reasons for their rejection or denial of some benefit. And as she suggests, if the machine won't tell you why your request was rejected, you have no basis for challenging that decision (Citron, 2008, p. 1277). Other, more direct challenges to the ontological authority being claimed by data scientists requires the development of a compelling demonstration of the fact that these algorithmic systems are not actually providing access to a previously hidden reality but are actually producing an alternative representation of that far more complex reality (Hildebrandt, 2018).

Fourteenth Amendment

The equal protection clause of the Fourteenth Amendment is identified as one constraint on the use of targeted surveillance of members of protected classes, despite the fact that proving

discriminatory intent is a significant challenge (Slobogin, 2002, p. 299). Recent evidence suggests that when there is an under-representation of minority group members on a community's police force, those agencies are more likely to use, or plan to use technology "that is designed for public surveillance, such that certain 'problem' or 'high risk' segments of the population can be better monitored" (Hendrix and Taniguci et al., 2018, p. 54). Of particular interest, in the face of suggestions that the US is actually moving toward enhanced surveillance of the entire population, this recent analysis suggests that African American racial asymmetry still remains the dominant influence over the use of surveillance technology in particular communities (Hendrix and Taniguci et al., 2018, p. 64).

An additional concern is that increasingly the risk-based assessments and identifications that are produced by algorithmic decision aids represent categories of persons outside that set of individuals traditionally entitled to equal protection (Hu, 2017). Although the algorithmic systems used to evaluate persons in terms of their criminal risk potential will be justified on the basis of the severity of the risks of concern, the claim that information about a subject's status as a member of a protected group played no role in the generation of their identification as suspicious, the disproportionality of the racial and ethnic inclusion among those targeted for heightened surveillance invites consideration of the role that race, ethnicity, religion and national origin actually played in the training of the algorithms (Hu, 2017, pp. 644-645).

More critically, as Hu (2017) suggests, the basis for many due process challenges seems likely to disappear as we move closer to that point in time when the "extreme vetting" experienced by immigrants, Muslims, and individuals with previous encounters with law enforcement agencies is better understood (Hu, 2017, p. 663) "as a function of database screening and digital watchlisting systems that can be applied equally to all citizens and noncitizens under a wide range of contexts, often justified by national and homeland security policy rationales." The fact is that the use of heightened scrutiny, guided by an algorithmic process, cannot be challenged as having been based on an intention to "discriminate on the basis of an impermissible classification" (Hu, 2017, p. 669). The remaining concern is that even if victims of illegitimate, or biased exclusionary classifications are harmed through this process, the counter-arguments from government agencies are likely to focus on the cumulative, or collective benefit to society that will be said to outweigh the harm to sets of individuals.

The privacy rights that are associated with the "freedom of self-determination and autonomy…fits well within the liberty category" (Crawford and Schultz, 2014, p. 111) that is covered in the due process clauses of both the Fifth and Fourteenth Amendments. In many of these cases, the nature of the concerns about due process are related to the nature of the "predictive privacy harms," and as they see it, the "greater the stigma or seriousness of the determination, the greater right one should have to question how Big Data adjudicated that result" (Crawford and Schultz, 2014, p. 118). Thus, in the case of predictive policing, it is argued that "the government would have to notify citizens that it was using predictive analytics and particular sets of public records to determine which areas of a city it marked as 'hot spots' as well as its capacity to determine if one lived or worked within the actual hot spots" (Crawford and Schultz, 2014, p. 126). The notification is related to the due process that would enable members of the public to examine both the data and the technology used to process it if they believed those determinations were erroneous.

Among the elements of due process with special meaning for decisions made within the CJS are those related to an individual's "right to be given notice of an agency's intended actions" in a timely fashion (Citron, 2008, p. 1281-2). This right to be given notice should apply to changes in the rules, but when the "rules" are changed through modification of the underlying software governing the operation of the automated decision-maker, such notifications are extremely rare. Exceptions to rules providing for public access to the source code, or rules governing a machine's processes are frequently based on "trade secret exemptions" claimed by the private corporations that provide the algorithms within their "black box" systems. But access to the mechanism, or even the logic behind the system's decision-making is routinely denied by government agencies (Citron, 2008, p. 1293). Citron's (2008, p. 1300) summary judgment about automation is quite clear: "Automation jeopardizes due process values, falsifies the central assumptions of administrative law, and subverts much of the social contract underlying the expansion of the administrative state."

The critical legal response

Scholarly assessments of the status of constitutional protections for anonymity, autonomy, and privacy are vitally important as contributions to an ongoing effort to reclaim them. Part of their value is the evidence and arguments that they make available to the public interest and advocacy organizations that attempt to modify the behavior of the courts through pressure focused on city, state and federal legislators by members of the public. The efforts of four organizations or partnerships are described in brief, and then followed by a scholarly effort that I hope will attract the attention of these and other activist groups willing to move us toward an engagement in an effort to reclaim reasonableness as a meaningful standard.

ACLU

In 2016, the American Civil Liberties Union (ACLU) initiated their Community Control Over Police Surveillance (CCOPS) effort in order mobilize the public to demand the passage of 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, 2017). The fact that they were able to report that eight cities had already passed bills incorporating many of the guiding principles behind their draft legislation, with an additional 20 cities currently engaged in the development of their own versions, including statewide drafts being developed in California and Maine, suggests that their initiative was both timely and well developed (ACLU, 2018). Indeed, in 2019, San Francisco led the way in banning the use of facial recognition technology by the police, despite the claims by the Police Officer's Association that "the ban would hinder their members' efforts to investigate crime" (Conger and Fausset, et al., 2019).

Electronic Frontier Foundation (EFF)

After delivering a withering criticism of the uses of facial recognition by law enforcement officers that included a harsh assessment of the inaccuracy and bias of the FBI's Interstate Photo

System and its FACE Services Unit, EFF's 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 as a result of the "over-collection of face recognition data," and the "current uncertainty of Fourth Amendment jurisprudence" in this area CJS (Lynch, 2017, pp. 23-26). Among the recommendations from EFF is an engagement with dangers that flow from the combination of multiple databases, including the merging of biometrics with a variety of contextual data in ways likely to increase the nature and extent of privacy harms. The final recommendation, and one that addresses the absence of a privacy commission in the US, is that government "entities that collect or use face recognition must be subject to meaningful oversight from an independent entity."

Leadership Conference on Civil and Human Rights and Upturn

The Leadership Conference on Civil and Human Rights and Upturn, a Washington, DC nonprofit seeking to promote "equity and justice in the design, governance, and use of digital technology" (Yu and Cook, et al., 2017) have developed a different set of standard policies and practices that they believe should be adopted by the nation's police departments. In 2017 they evaluated 75 local police departments around the nation, focusing their attention on the departments in the major cities, as well as those departments 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 satisfied those criteria. Among the eight evaluative criteria used in this scorecard, those with particular relevance to questions being raised by members of the most often recorded populations are whether policies: 1) limit officer discretion on when to record; 2) address personal privacy concerns; 3) prohibit officer pre-report viewing; 4) protects footage against tampering and misuse; 5) makes footage available to individuals filing complaints; and 6) limits biometric searching of footage (Yu, et al., 2017, pp. 6-7). Not all of the frequently expressed public concerns about the use of BWCs were included among these eight criteria (Zwart, 2018). Among the blind spots in this list are those related to the privileged access to the recordings that is reserved to the police and prosecutors, that places criminal defendants at a significant procedural disadvantage. They 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," and they reported that the "vast majority of departments (55) allow officers unrestricted footage review." (Yu and Cook, et al., 2017, pp. 8-9).

In search of reasonableness

In his engagement with the challenges involved in realizing some degree of algorithmic accountability Binns (2018, p. 550) suggests that "public reason could act as a constraint on algorithmic decision-making power be ensuring that decision-makers must be able to account for their system's outputs according to epistemic and normative standards which are acceptable to all reasonable people."

Unfortunately, Binns avoids specifying which source of evidence we should rely upon to provide a measure of public reason. Although it is likely to be seen as an unrealistic demand, Chao and

her colleagues (2018) suggest that the courts should rely more on well-designed surveys and experiments to gain a better understanding of what the public actually feels about surveillance and algorithmic decision-making. Beginning with a comprehensive review of past research, and a sophisticated survey-based experiment, Chao and Durso, et al., (2018) reveal the extent to which judges' intuitions about privacy do not reflect the views held by substantial segments of the population, especially with regard to the manner in which police take advantage of the third party doctrine to access information that the courts have said the public cannot reasonably treat as private.

On the basis of comparisons of the rankings of severity established by Supreme Court decisions, they conclude that the contemporary public considers "every one of the 'technology searches' to be more intrusive of privacy than actions that the Court has held does violate reasonable expectations of privacy" (Chao and Durso, et al., 2018, p.309). Indeed, the general public apparently views five of several technologically enabled searches to be more intrusive than a search by the police of someone's bedroom—the kind of search that has historically anchored the extreme end of the Court's views about privacy.

While the departures of the contemporary public's ranking of intrusiveness from that of the Supreme Court are substantial, even greater differences are observed when comparisons are made with populations defined by race and experience with law enforcement. African Americans and those identifying as "other" ranked more scenarios as violations of reasonable expectations of privacy than whites (Chao and Durso, 2018, pp. 310-311). Because of their experiences over time with law enforcement, African Americans tend to have less trust, and apply lower levels of legitimacy to policing in their communities (Hendrix and Taniguchi, et al., 2018).

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 that they invite us to understand as a new form of colonialism, they see the recognition of this process as the first step we have to take in order to mount the kinds of resistance that the circumstances demand. The efforts of the ACLU, the Leadership Forum, Upturn and EFF will need to be expanded, and replicated at the local, state, national and international levels, especially with regard to the need to establish independent agencies for which the legislative and judicial supports for the misappropriation and exploitation of TGI would be identified as primary targets for reversal. And finally, the reconstitution of an agency with a mission like that of its predecessor, the US Office of Technology Assessment, will be an essential step toward overcoming an addiction to technological developments that threaten, rather than advance the human condition (Graves and Kosar, 2018).

References

(ACLU), A. C. L. U. (2017). 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.

Ananny, M. and K. Crawford (2016). "Seeing without knowing: Limitations on the transparency ideal and its application to algorithmic accountability." new media & society: 1-17.

Atzori, L., A. Iera, et al. (2010). "The Internet of Things: A survey." Computer Networks 54(15): 2787-2805.

Barocas, S. and A. D. Selbst (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, L. P. (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*. Washington, DC, The Aspen Institute: 58.

Bowker, G. C. and S. L. Star (1999). *Sorting Things Out: Classification and its consequences*. Cambridge, MA, The MIT Press.

Brakel, R. V. and P. D. Hert (2011-3). "Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies." *Cahiers Politiestudies* (nr.20): 163-192.

Brauneis, R. and E. P. Goodman (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.

Burr, C. and N. Cristianini (2019). “Can machines read our minds?” *Minds & Machines*, https://doi.org/10.1007/s11023-019-09497-4

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

Campolo, A., M. Sanfilippo, M. Whittaker, K. Crawford. *AI Now 2017 Report*. New York: AI Now Institute at New York University.

Carney, R. K. and R. D. Enos (2017). *Conservatism and fairness in contemporary politics: Unpacking the psychological underpinnings of modern racism*. NYU CESS Experiments Conference. New York City.

Chao, B., C. Durso, et al. (2018). "Why courts fail to protect privacy: Race, age, bias, and technology." *California Law Review* 106(2): 263-324.

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

Citron, D. K. (2008). "Technological due process." *Washington University Law Review* 85(6): 1249-1313.

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

Cohen, J. E. (2017b). *Surveillance vs. privacy: Effects and implications. Cambridge Handbook of Surveillance Law*. D. Gray and S. E. Henderson (eds). New York, Cambridge University Press: 455-469.

Cohen, J. E. (2019). "Turning privacy inside out." *Theoretical Inquiries in Law* 20.1. (forthcoming). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3162178

Conger, K., R. Fausset and S.F. Kovaleski (2019). “San Francisco bans facial recognition technology.” *New York Times* (May 14). https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html

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

Couldry, N. and U. A. Mejias (2019). “Data colonialism: Rethinking big data’s relation to the contemporary subject.” *Television & New Media* 20(4): 336-349. https://doi.org/10.1177/1527476418796632

Crawford, K. and J. Schultz (2014). "Big data and due process: Toward a framework to redress predictive data harms." *Boston College Law Review* 55(1): 93-128.

Davies, W. (2017). "How are we now? Real time mood-monitoring as valuation." *Journal of Cultural Economy* 10(1): 34-48.

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

Degeling, M., C. Utz, C. Lentzsch, H. Hosseini, F. Schaub and T. Holz (2019). *We value your privacy… Now take some cookies: Measuring the GDPRs impact on web privacy*. Network and Distributed Systems Security Symposium 2019. San Diego, CA, NDSS.

Ferguson, A. G. (2012). "Predictive policing and reasonable suspicion." *Emory Law Journal* 62: 259-325.

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

Ferguson, A. G. (2017). "Policing predictive policing." *Washington University Law Review* 94(5): 1115-1194.

Ferguson, A. G. (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. (September 26) *The Atlantic*. https://www.theatlantic.com/technology/archive/2018/09/body-camera-police-future/571402/

Gandy, O. H. (2000). "Exploring identity and identification in cyberspace." *Notre Dame Journal of Law, Ethics & Public Policy* 14(2): 1085-1111.

Gandy, O. H. (2006). Data mining, surveillance, and discrimination in the post-9/11 environment. *The New Politics of Surveillance and Visibility*. K. Haggerty and R. V. Ericson (eds), Toronto, University of Toronto Press: 363-384.

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

Gandy, O. H. (2012). “Statistical surveillance: Remote sensing in the digital age.” *Routledge Handbook of Surveillance Studies*. K. Ball, K. D. Haggerty and D. Lyon (eds). New York, Routledge: 125-132.

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

Gelles, D. (2016). “Taser International dominates police body camera market.” (July 13) *New York Times*. https://www.nytimes.com/2016/07/13/business/taser-international-dominates-the-police-body-camera-market.html

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

Goldenfein, J. (2018). “The Profiling Potential of Computer Vision and the Challenge of Computational Empiricism” (November 14, 2018). *Proceedings of the 2019 ACM FAT* Conference,* Forthcoming. https://ssrn.com/abstract=3284598

Graves, Z. and K. Kosar (2018). *Bring in the Nerds: Reviving the Office of Technology Assessment.* R Street Policy Study No. 128. Washington, DC: R Street. https://www.rstreet.org/wp-content/uploads/2018/01/Final-128.pdf

Greene, D., A. L. Hoffman and L. Stark (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.

Greene, D. and G. Patterson (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).

Hayes, R. M. (1993). Measurement of information and communication: A set of definitions. In J. R. Schement and B. D. Rubin (eds). *Between Communication and Information*. Information and Behavior, Vol. 4. New Brunswick, NJ, Transaction Publishers: 81-103.

Hendrix, J. A., T. A. Taniguchi, K. J. Strom, K. Barrick and N. J. Johnson (2018). "The eyes of law enforcement in the new panopticon: Police-community racial asymmetry and the use of surveillance technology." *Surveillance & Society* 16(1): 53-68.

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

Joh, E. E. (2016 a). "Policing by the numbers: Big data and the fourth amendment." *Washington Law Review* 89: 35-68.

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

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

Kampfe, K. (2015). "Police-worn body cameras: Balancing privacy and accountability through state and police department action." *Ohio State Law Journal* 76(5): 1153-1200.

Kim, P. T. (2017). "Data-driven discrimination at work." *William & Mary Law Review* 58(3): 857-936.

Knight, W. (2017). “The dark secret at the heart of AI: No one really knows how the most advanced algorithms do what they do. That could be a problem.” *MIT Technology Review*: 1-17.

Kroll, J. A., J. Huey, S. Barocas, E. W. Felton, J. R. Reidenberg, D. G. Robinson and H. Yu (2017). "Accountable algorithms." *University of Pennsylvania Law Review* 165: 633-705.

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.” *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination.* D. Lyon (ed). New York, Routledge: 13-30.

Maharrey, M. (2018). *How federal surveillance and "parallel construction" undermine the rule of law*. Los Angeles, CA, Tenth Amendment Center.

Manovich, L. (2018). "100 billion data rows per second: Media analytics in the early 21st century." *International Journal of Communication* 12: 473-488.

Mateescu, A., A. Rosenblat and d. boyd (2015). “Police body-worn cameras.” Data and Society Research Institute. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2569481

Maurer, D. (2017). Testimony. “Face Recognition Technology: DOJ and FBI need to take additional actions to ensure privacy and accuracy.” House Committee on Oversight and Government Reform. U. S. Government Accountability Office, GAO-17-489T.

McPhail, B., A. Clement, J. Ferenbok and A. Johnson (2013). “‘I'll be watching you’: Awareness, consent, compliance and accountability in video surveillance.” IEEE International Symposium on Technology and Society, Toronto, ON, Canada.

Metcalf, J. and K. Crawford (2016). "Where are the human subjects in Big Data research? The emerging ethics divide." *Big Data & Society*: 1-14.

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

Nakar, S. and D. Greenbaum (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.

Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA, Stanford University Press.

Obama, B. (2017). *The president's role in advancing criminal justice reform*. U.S. Department of Justice Publication and Materials, Digital Commons & University of Nebraska.

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.

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

Rieke, A., M. Bogen and D. G. Robinson (2018). *Public scrutiny of automated decisions: Early lessons and emerging methods*, Washington, DC: Upturn, and Omidyar Network.

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

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

Schmidt, C. (2019). “Sheriff renews push for funds tied to border.” *Arizona Daily Star*. Tucson, AZ: 1-2.

Selbst, A. (2019). "Negligence and AI's human users." *Boston University Law Review*, Forthcoming.

Selbst, A. D. (2017). "Disparate impact in big data policing." *Georgia Law Review* 52: 109-195.

Selbst, A. D., D. Boyd, S. A. Friedler, S. Venkatasbramanian and J. Vertesi (2019). "Fairness and abstraction in sociotechnical systems." 2019 ACM Conference on Fairness, Accountability, and Transparency. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3265913.

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

Solove, D. J. and M. Rotenberg (2003). *Information Privacy Law*. New Yok, Aspen Publishers.

Steinbock, D. J. (2004). "National identity cards: Fourth and Fifth Amendment issues." *University of Florida Law Review* 56(4): 698-760.

Turow, J., M. Hennessy, N. Draper, O. Akanbi and D.Virgilio. (2018). *Divided we feel: Partisan politics drive Americans' emotions regarding surveillance of low-income populations*. Philadelphia, PA: Annenberg School for Communication.

Weisburd, D. and M. K. Majmundar, 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.

Whittaker, M., K. Crawford, et al. (2018). *AI Now Report 2018*. New York, AI Now Institute, New York University: 62.

Winston, A. (2018). "Palantir has secretly been using New Orleans to test its predictive policing technology." *The Verge*.

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

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

Zhang, Z. and D. B. Neill (2017). “Identifying significant predictive bias in classifiers.” 2017 Workshop on Fairness, Accountability, and Transparency in Machine Learning. arXiv preprint arXiv:1611.08292, 2016 - arxiv.org

Zwart, W. (2018). "Slow your roll out of body-worn cameras: Privacy concerns and the tension between transparency and surveillance in Arizona." *Arizona Law Review* 60(3): 783-814.