

6-1-2019

## Can We Trust Artificial Intelligence in Criminal Law Enforcement?

Sara M. Smyth

*Faculty of Law, Latrobe Law School*

Follow this and additional works at: <https://digitalcommons.schulichlaw.dal.ca/cjlt>



Part of the [Internet Law Commons](#), and the [Science and Technology Law Commons](#)

---

### Recommended Citation

Sara M. Smyth, "Can We Trust Artificial Intelligence in Criminal Law Enforcement?" (2019) 17:1 CJLT 99.

This Article is brought to you for free and open access by the Journals at Schulich Law Scholars. It has been accepted for inclusion in Canadian Journal of Law and Technology by an authorized editor of Schulich Law Scholars. For more information, please contact [hannah.steeves@dal.ca](mailto:hannah.steeves@dal.ca).

**NOTE:**  
**Can We Trust Artificial Intelligence in Criminal Law  
Enforcement?**

Sara M. Smyth\*

**INTRODUCTION**

Artificial intelligence (AI), sometimes called machine intelligence, is intelligence demonstrated by machines — or computer systems — able to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision-making and language translation. Most of us are already accustomed to using AI in all sorts of areas of our lives, such as when we use our smartphones or when we ask Alexa — Amazon’s voice-control system — a question, or issue a command.

With the help of AI, voice-enabled devices like Amazon Echo [*i.e.* “Alexa”] are enabling the very sort of sci-fi interactions we’ve long extolled — think of the onboard conversational computer that ran the U.S.S. *Enterprise* in *Star Trek*, answering the crew’s requests.<sup>1</sup> Now, we live in a world where computers really can understand conversational speech and make our lives easier by doing a wide range of things for us. We can walk into a dark room and ask for the lights to be turned on; or, wake up and ask for a pot of coffee to be made. We can ask Alexa about the weather, find recipes, get help with a math problem, order products online, make restaurant reservations and call an Uber — all without touching anything.<sup>2</sup>

With the rapid advances made by AI in the last few years, yet with so much of it happening behind the scenes, it’s no wonder that most people are both baffled and awestruck by the capacity for these systems to render humans obsolete. Until recently, much of what the general public knew about AI, robotics, and their superhuman capabilities came from Hollywood blockbuster films like *Minority Report*. While it’s true that these films, in fact, provided a surprisingly realistic portrait of the capabilities that AI can now deliver, there is still a real lack of understanding on the part of most people about the profound effects of AI upon the way we operate as a society.

With the ability to walk into a room and simply say “lights on,” it’s apparent that we don’t need to think much about AI in the context of our routine tasks as

---

\* Associate Professor, LaTrobe Law School, Melbourne.

<sup>1</sup> Khari Johnson, “How ‘Star Trek’ inspired Amazon’s Alexa” *Venturebeat* (7 June 2017) online: < [venturebeat.com/2017/06/07/how-star-trek-inspired-amazons-alexa/](http://venturebeat.com/2017/06/07/how-star-trek-inspired-amazons-alexa/) > .

<sup>2</sup> Grant Clauser, “What Is Alexa? What Is the Amazon Echo, and Should You Get One?” *Wirecutter* (29 January 2019) online: < [thewirecutter.com/reviews/what-is-alexa-what-is-the-amazon-echo-and-should-you-get-one/#how-does-alexa-work](http://thewirecutter.com/reviews/what-is-alexa-what-is-the-amazon-echo-and-should-you-get-one/#how-does-alexa-work) > .

we go about our daily lives. Yet, there are important questions to be asked around transparency, accountability and whether we can even trust AI's invasion of our lives in the first place.

Recent research has uncovered the dangers of hidden bias in AI systems. These biases can lie in the data, algorithms, and the overall design of the systems themselves, as well as the credibility and weight assigned to their findings.<sup>3</sup> The introduction of such bias should raise alarm bells when applied to a criminal justice system that has already long imposed disproportionate burdens on racial minorities and the poor.

Predictive algorithms, risk models, and other sorts of automated decision-making tools are now ubiquitous in the public service.<sup>4</sup> Investments in these systems are often justified by calls for administrative efficiency — doing more with less and making decisions on a fairer and more consistent basis. They have become powerful tools of social categorization, facilitating discrimination between different populations through what are often vague and spurious modes of classification. In many cases, they reinforce unjust stereotypes that are already far too common in our criminal justice system. They are powerful forces for control, manipulation and punishment, which can restrict people's civil liberties and undermine their civil rights.<sup>5</sup>

## TRANSPARENCY, ACCOUNTABILITY & TRUST

Imagine a world where police can predict a crime before it happens. It's already the stuff of science fiction and Hollywood: recall Philip K. Dick's short story turned movie *Minority Report*, in which there is a special government branch in New York, in the year 2054, called "Precrime" that apprehends those who have been identified by three mutants — or "precogs" — as committing murders in the future. While this is clearly fiction, police departments are increasingly deploying data mining techniques to predict, prevent, and investigate crime. But should we trust AI to decide who is a criminal and what defines a crime?

From a law enforcement perspective, anonymity is the enemy. The need to "de-anonymize" the individual has long been central to solving crime. Increasingly, this function is being undertaken by technology that augments or replaces human capabilities altogether. Body cameras and smart glasses worn by law enforcement are now being integrated with facial recognition and other artificial intelligence tools, including automated analytics and database screening capacities. As technologies progress, they are likely to be used to link biometric identity to multidimensional surveillance (*e.g.*, algorithmic-driven biographical

---

<sup>3</sup> Elizabeth E. Joh, "Artificial Intelligence and Policing: First Questions" (2018) 41 Seattle U.L. Rev. 1139, online: <papers.ssrn.com/sol3/papers.cfm?abstract\_id=3168779>.

<sup>4</sup> Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (New York: St. Martin's Press, 2018) at 9.

<sup>5</sup> *Ibid* at 10.

screening and behavioural analysis).<sup>6</sup> Body cameras may also one day be used to assess future risk and isolate other data deemed suspicious.<sup>7</sup>

The other trend is the deployment of AI with object detection, crowd monitoring, and feature extraction to filter, collect, and analyze the data and create detailed profiles about individuals. The technology can detect people walking down the street and offer information about their identities, including their name, job, and online public profiles. The goal is to track and monitor where people are at all times of the day and night, what they're doing, who they associate with, and what they believe.<sup>8</sup> It means that just by having a snapshot of someone, they suddenly have their entire identity.

At the same time, the reliance upon AI and the collection of vast amounts of information poses challenges for law enforcement and the courts. Digital policing creates a number of well-known concerns; and it can also increase the privacy and civil liberties intrusions borne by law-abiding citizens. It can lead the police to focus on detecting crimes committed by certain populations and in certain locations, giving rise to concerns about racial and class bias.

Cities such as Los Angeles, Atlanta, Santa Cruz, and Seattle have used software to predict where property crimes will occur.<sup>9</sup> In Charlotte, North Carolina, police compiled foreclosure data to generate a map of high-risk areas that are likely to be struck by crime.<sup>10</sup> In New York City, the N.Y.P.D. has partnered with Microsoft to employ a “Domain Awareness System” that collects and links information from various sources like CCTVs, licence plate readers, radiation sensors, and informational databases.<sup>11</sup>

The use of predictions in policing is not new. Crime mapping, which allows the police to allocate more resources to where crime is most likely to occur, has been around for a very long time; and, police used to plot crime on a map — with different coloured pins representing various crimes — to see if hot spots emerged.<sup>12</sup> Today's crime-mapping technologies can produce nearly perfect information about the frequency and geographic location of crimes in any given area.<sup>13</sup> Some jurisdictions have almost real-time data collection and daily reports of problematic areas to officers in the field.<sup>14</sup>

---

<sup>6</sup> Margaret Hu, “Bulk Biometric Metadata Collection” (2018) 96 N.C. L. Rev. 1425 at 1435.

<sup>7</sup> *Ibid* at 1435.

<sup>8</sup> Simon Denyer, “China’s Watchful Eye” *The Washington Post* (7 January 2018).

<sup>9</sup> Andrew D. Selbst, “Disparate Impact in Big Data Policing” (2017) 52 Ga. L. Rev. 109 at 114.

<sup>10</sup> Joh, *supra* note 3 at 35.

<sup>11</sup> *Ibid* at 35.

<sup>12</sup> Andrew Guthrie Ferguson, “Crime Mapping and the Fourth Amendment: Redrawing High-Crime Areas” (2011) 63 Hastings L.J. 179 at 184.

<sup>13</sup> *Ibid* at 182.

<sup>14</sup> *Ibid*.

Other systems use social network analysis to determine which persons are at a high risk of becoming the victims or perpetrators of violence. Just like crime mapping, offender profiling, in which police examine psychological and environmental factors to predict an unknown suspect's identity or to anticipate the next crime, is another form of prediction that has been around for a very long time. The algorithms themselves are largely secret, but the factors include past criminal history, arrests, parole status, and whether the target has been identified as part of a gang. The algorithm ranks these variables to come up with a predictive score of how "hot" individuals might be in terms of their risk.

The premise behind profiling is that a significant portion of crime occurs in predictable patterns, and if police can find those patterns, they can either prevent crime or catch the criminals.<sup>15</sup> While these predictive technologies are novel, the concerns underlying them are antiquated.<sup>16</sup> Fears of racial bias, a lack of transparency, data error, and the distortions of constitutional protections offer serious challenges to the development of workable predictive policing approaches. There are actually *two* separate problems at issue: the fact that predictive policing systems have the potential for discriminatory results; and, the lack of awareness about the efficacy and discriminatory impact of these systems.<sup>17</sup>

Data mining is the process of using machine learning to find patterns and relationships among different people or outcomes.<sup>18</sup> It works by exposing a machine learning algorithm to examples of cases with known outcomes.<sup>19</sup> The system then builds a predictive model — a set of correlations that determine which associated attributes can serve as useful proxies for an otherwise unobservable outcome.<sup>20</sup> Once those attributes are discovered, the system compares new subjects' traits to those observed attributes to make predictions about the outcome.

Yet, data mining systems also incorporate a series of human-made decisions that can create or exacerbate discriminatory outcomes, independent of any intent to do so.<sup>21</sup> For example, some use data about past criminal activity, such as crime locations and arrest records. In other cases, data mining companies purchase tools "largely developed by and for the commercial world," as well as data from social networks such as Facebook and Twitter.<sup>22</sup>

When police allocate more resources to areas where there has been more crime in the past, crimes in those areas will be over-represented in future data.<sup>23</sup>

---

<sup>15</sup> Selbst, *supra* note 9 at 126.

<sup>16</sup> Ferguson, *supra* note 12 at 380.

<sup>17</sup> Selbst, *supra* note 9 at 168.

<sup>18</sup> *Ibid* at 127.

<sup>19</sup> *Ibid*.

<sup>20</sup> *Ibid*.

<sup>21</sup> *Ibid* at 116.

<sup>22</sup> *Ibid* at 128.

Furthermore, when predictive policing is used to decipher where to put more officers, this creates a “positive feedback loop” that skews future data, as the increased police presence will lead to the detection of more crime in that area.<sup>24</sup> These systems can also lead to extra monitoring of individuals, and when a crime occurs, police might be more likely to look at them first.<sup>25</sup>

Over time, the appearance of greater threat levels in minority neighbourhoods could inflame an already adversarial relationship with police and put lives at risk. For example, increased police presence means a greater likelihood of police-citizen encounters. If a high percentage of stop and frisks turn out to be erroneous, this results in an unnecessary infringement on personal liberty.<sup>26</sup> Whether they view this as a helpful presence or reject it as an unnecessary interference with their liberty, residents in these areas are forced endure ongoing police surveillance as an ever-present daily reality.<sup>27</sup> The perception of mistreatment only undermines the legitimacy of the front-line responders in these areas.<sup>28</sup>

In August 2016, 17 civil rights organizations released a joint statement on the civil rights concerns of predictive policing, emphasizing the possibility of racist outcomes, as well as the lack of transparency, public debate, and attention to community needs.<sup>29</sup> The way police are using these technologies means more people of colour are arrested, jailed, or physically harmed by police, while the needs of communities are often ignored. We must keep in mind that policing is different from other fields that have embraced AI because the police act with enormous discretion: they choose where to focus their attention, whom to detain, arrest, and even when to use deadly force.<sup>30</sup> The type of AI utilized thus has significant implications for both power and accountability in policing.

Since all humans exhibit unconscious bias, it’s clear that police officers do too. The fact of unconscious bias is widely acknowledged; and, thus, it seems to make good sense to take at least some discretion away from unreliable human officers and give it to a seemingly neutral technology. Yet, researchers have found that “seemingly objective” algorithms can reproduce the very same biases of the engineers who designed them — not to mention the officers who are tasked with using them on the street.

Knowledge of crime patterns in a particular area can make an officer’s observations appear more reasonable where that knowledge is tied to the suspicion of the observed person.<sup>31</sup> However, if the reference to a high-crime area

---

<sup>23</sup> Selbst, *supra* note 9 at 135.

<sup>24</sup> *Ibid.*

<sup>25</sup> *Ibid* at 137.

<sup>26</sup> Ferguson, *supra* note 12 at 217.

<sup>27</sup> *Ibid.*

<sup>28</sup> *Ibid* at 228.

<sup>29</sup> Selbst, *supra* note 9 at 114.

<sup>30</sup> Joh, *supra* note 3.

weighs in favour of reasonable suspicion, this means that the same activity in one neighbourhood (*i.e.* a high-crime area), but not in another (*i.e.* a low-crime area), may rise to the level of reasonable suspicion. Yet, the same objective standard of reasonable suspicion is assumed to apply in *all* neighbourhoods and to *all* people.<sup>32</sup> Furthermore, some courts have expressed concern or confusion about what a high-crime area is, or how it should be weighed against other factors in the reasonable suspicion analysis; and, courts have developed different standards and solutions to resolve the issue.<sup>33</sup> This raises fairness concerns, including “issues of race, class, and place”.<sup>34</sup>

New high-tech tools allow for more precise measuring and tracking, better sharing of information, and the possibility of identifying racial bias. In a perfect world, automated decision-making could be used to apply the rules in each case consistently and without prejudice. With this aim, data-driven risk assessment tools are being used to set bail, determine sentences, and even contribute to determinations about guilt or innocence.

These systems operate on the basis that a data subject’s expected outcome for some query is similar to other people with whom he or she shares relevant attributes, like age, sex, geography, family background, and employment status. As a result, two people accused of the same crime may receive different bail or sentencing outcomes based on inputs that are beyond their control, and which they have no way of assessing or challenging. As criminal justice algorithms have come into more widespread use, they have also come under greater scrutiny. They have been criticized for being unclear, unreliable, and even unconstitutional. It’s evident, for example, that risk assessment scores used in criminal sentencing overestimate black recidivism and underestimate white recidivism.<sup>35</sup>

Another example of AI at work in the criminal justice system is the use of algorithms to decide a defendant’s potential recidivism. Courts across the United States are already using this tool. There are a lot of factors that go into making the determination and the exact formula is proprietary. What we do know is that the technology promises to bring uniformity, fairness and scientific discipline to an area of law that has always been arbitrary and capricious.

---

<sup>31</sup> In *Pennsylvania v. Dunlap*, 129 S. Ct. 448 (U.S. Sup. Ct.,2008), for example, the officer staked out a particular location with a specific crime problem because of an official decision of his police administrators; and, the expected type of criminal activity matched what Officer Devlin actually saw - suspected narcotics dealing.

<sup>32</sup> Ferguson, *supra* note 12 at 199.

<sup>33</sup> *Ibid* at 203.

<sup>34</sup> *Ibid* at 206.

<sup>35</sup> Julia Angwin et al., “Machine Bias: There’s Software Used Across the Country to Predict Future Criminals. And It’s Biased Against Blacks”, *ProPublica* (23 May 2016) online: <<https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>> .

Proponents argue the software is ground breaking and revolutionary. More importantly, an algorithm isn't biased. It appears to be efficient, precise, and immune to lapses in judgment. Yet many have argued that the data is biased — it sentences African-Americans and Latinos disproportionately to whites for the same crimes. Yet, so do judges. So, the algorithm is said to be an improvement — a check on an already flawed system. But the algorithm has no historical context. It can't account for the factors that influence disproportionately higher rates of incarceration for minorities across the United States.

The Correctional Offender Management Profiling for Alternative Sanctions, or COMPAS, created by the for-profit company Northpointe, aims, and claims, to predict an individual's risk of recidivism. It assesses variables under five main areas: criminal involvement, relationships/lifestyles, personality/attitudes, family, and social exclusion. In addition, it evaluates nearly two dozen so-called "criminogenic needs" that relate to the major theories of criminality, including "criminal personality," "social isolation," "substance abuse" and "residence/stability". Defendants are ranked low, medium or high risk in each category. Although these risk categories may be presented in "neutral" language, often moral evaluations — judgments about who is good and who is bad — are hidden in the technical wording; and, riskiness is assessed behind the scenes, by secret algorithms.<sup>36</sup>

Nevertheless, the use of such algorithms in risk assessment is becoming increasingly common in courtrooms across the United States. They are being used to make decisions about who can be released at every stage of the criminal justice system, from assigning bail amounts — as is the case in Fort Lauderdale — to even more significant decisions about defendants' liberty. In Arizona, Colorado, Delaware, Kentucky, Louisiana, Oklahoma, Virginia, Washington, and Wisconsin, the results of such assessments are given to judges during criminal sentencing.

Not only do these techniques largely do away with judicial discretion in sentencing matters, they compound racially based harms because they are used to determine an offender's propensity for recidivism based on attributes held by *other* people. In other words, the data relied on to determine a particular offender's level of risk is comprised of the recidivism rates collected from multiple sample populations of released offenders for a specific period of time.

COMPAS then compares the offender's information with the group data to generate a "risk score" meant to predict the likelihood that those with a similar history of offending are either more or less likely to commit another crime following release from custody. Moreover, since the system not only measures risk, but a variety of other vague and spurious criteria, including, "criminal personality," "social isolation," "substance abuse" and "residence/stability," the results can easily be prone to misinterpretation and manipulation, not to mention false positives.

<sup>36</sup> Colin J. Bennett et al., eds., *Transparent Lives: Surveillance in Canada (The New Transparency Project)* (Edmonton: Athabasca University Press, 2014) at 47.

Wisconsin has been among the most eager and expansive users of Northpointe's risk assessment tool in sentencing decisions. In 2012, the Wisconsin Department of Corrections launched the use of the software throughout the state. It is now used at each step in the prison system, from sentencing to parole. Once a defendant is convicted of a felony anywhere in the state, the Department of Corrections attaches a COMPAS assessment to the confidential pre-sentence report given to judges.<sup>37</sup>

On August 12, 2013, Circuit Court Judge Scott Horne in La Crosse County, Wisconsin, relied on the defendant Eric Loomis's COMPAS assessment as one of several factors when deciding his sentence. As part of his explanation for the sentence, Judge Horne stated: "You're identified, through the COMPAS assessment, as an individual who is at high risk to the community. In terms of weighing the various factors, I'm ruling out probation because of the seriousness of the crime and because your history, your history on supervision, and the risk assessment tools that have been utilized, suggest that [you're] extremely high risk to reoffend."<sup>38</sup> He then imposed a sentence of eight years and six months in prison.

Loomis, who was charged with driving a stolen vehicle and fleeing from police, challenged the sentencing court's reliance on the COMPAS assessment as a violation of his due process rights because he could not contest the scientific validity of the assessment due to Northpointe's proprietary claim over the software's algorithm.<sup>39</sup> The Court of Appeals of Wisconsin certified an appeal to the Supreme Court of Wisconsin, noting that: "the lack of transparency regarding COMPAS appears to present a unique sentencing situation and, therefore, is suitable for supreme court review".<sup>40</sup>

On appeal to the Supreme Court of Wisconsin,<sup>41</sup> the state opposed Loomis's request for a resentencing hearing and defended the use of the COMPAS score on the basis that judges can consider it in addition to other factors. The Court agreed and held that: ". . . because the circuit court explained that its consideration of the COMPAS risk scores was supported by other independent factors, its use was not determinative in deciding whether Loomis could be supervised safely and effectively in the community. Therefore, the circuit court did not erroneously exercise its discretion."<sup>42</sup>

Indeed, the circuit court "considered multiple factors that supported the sentence it imposed," particularly, "the seriousness of the crime and Loomis's criminal history . . . [which] . . . both bear a nexus to the sentence imposed".<sup>43</sup>

---

<sup>37</sup> *Ibid.*

<sup>38</sup> *State v. Loomis*, 2015 Wisc. App. LEXIS 722, 2-4, 2015 WL 5446731 at 4.

<sup>39</sup> *Ibid* at 4-6.

<sup>40</sup> *Ibid* at 6.

<sup>41</sup> *State v. Loomis*, 2016 WI 68, 371 Wis. 2d 235, 881 N.Q.2d 749, 2016 Wisc. LEXIS 178.

<sup>42</sup> *Ibid* at 9.

<sup>43</sup> *Ibid* at 84-86.

This is consistent with the principle that the court should consider many factors in sentencing, including “the past record of criminal offenses, history of undesirable behavior patterns, and results of presentence investigation”.<sup>44</sup> Thus, the court concluded that the use of the COMPAS risk assessment at sentencing did not violate Loomis’s right to due process.<sup>45</sup>

The attractiveness of a system like COMPAS is that it purports to inject objectivity into a criminal justice system that has been compromised, far too many times, by human error through bias, racism, xenophobia, stereotyping, and discrimination. However, this seemingly compelling solution overlooks the fact that algorithms, their “science” notwithstanding, are as fallible as the people, and the institutions, that write them.<sup>46</sup> Furthermore, if private companies like Northpointe can keep their algorithms confidential, by claiming that they are trade secrets, no one will ever truly know how the system calculates risk.

When mental health professionals and other experts give evidence in court about an offender’s risk of reoffending, they are typically cross-examined, and this process provides an opportunity to test the evidence for the truth of its contents, as well as to question the credibility of the witness. Yet, since a software program, like COMPAS, can never be examined or deposed — and neither can its makers be compelled to reveal the “trade secrets” behind their methods — there is the obvious potential for juries and judges to misunderstand and misuse the results, assigning greater accuracy to predicted outcomes than is warranted.<sup>47</sup> As well, such risk assessments classify individuals within a group as low, medium or high risk; yet, they cannot say exactly where in this group the individual lies, and therefore cannot pinpoint the precise risk the individual poses.<sup>48</sup>

Assigning risk to an individual based on group characteristics can lead to inaccurate assessments; and, if these inaccuracies cannot be teased out through cross-examination, this has the practical effect of turning a tool for the assessment of probabilities for future offending into something relied on as empirically infallible. That seems to upend principles of due process, fairness, and the right of the defendant to make full answer and defence. This is particularly true given that these tools give scientific value to estimations that actually perform less well than chance.<sup>49</sup>

In fact, research carried out by ProPublica demonstrated that the results produced by COMPAS *are* dubious and racially biased against minorities. They obtained the risk scores assigned to more than 7,000 people arrested in Broward

<sup>44</sup> *Ibid* at 85. See also *State v. Gallion*, 270 Wis. 2d 535 and *Harris v. State*, 75 Wis. 2d 513, 519, 250 N.W.2d 7 (1977).

<sup>45</sup> *Ibid* at 86.

<sup>46</sup> Megan Garber, “When Algorithms Take the Stand” *The Atlantic* (30 June 2016).

<sup>47</sup> Bernadette McSherry & Patrick Keyzer, *Sex Offenders and Preventive Detention: Politics, Policy and Practice* (Leichhardt, NSW: The Federation Press, 2009) at 33.

<sup>48</sup> *Ibid* at 30.

<sup>49</sup> Frank R. Farnham & David V. James, “Dangerousness and Dangerous Law” (2001) 358 *The Lancet* 1926 at 1926.

County, Florida, in 2013 and 2014 and checked to see how many were charged with new crimes over the next two years, the same benchmark used by the creators of the algorithm. The score proved unreliable in forecasting violent crime: only 20 percent of the people predicted to commit violent crimes actually went on to do so. When a full range of crimes were considered — including misdemeanors such as driving with an expired licence — the algorithm was just slightly more accurate than a coin toss. Of those deemed likely to reoffend, only 61 per cent were arrested for a subsequent crime within two years.

ProPublica also uncovered significant racial disparities. In forecasting who would reoffend, the algorithm made mistakes with African-American and white defendants at roughly the same rate but in very different ways: the system was particularly likely to falsely flag African-American defendants as future criminals, wrongly labelling them this way at almost twice the rate as white defendants; and white defendants were mislabeled as low risk more often than African-American defendants. African-American defendants were 77 per cent more likely to be pegged at higher risk of committing a future violent crime and 45 per cent more likely to be predicted to commit a future crime of any kind than whites. Thus, not only may these risk scores be injecting bias into the courts that use them, they may also be inflaming unfair disparities.

Notably, despite ruling against *Loomis*, even the Wisconsin Supreme Court seemed uneasy about using a secret algorithm to send a man to prison. Justice Ann Walsh Bradley, writing for the court, discussed the ProPublica report about COMPAS: “[a] recent analysis of COMPAS’s recidivism scores based upon data from 10,000 criminal defendants in Broward County, Florida, concluded that black defendants ‘were far more likely than white defendants to be incorrectly judged to be at a higher risk of recidivism.’ Likewise, white defendants were more likely than black defendants to be incorrectly flagged as low risk.”<sup>50</sup> She further observed that, “this study and others raise concerns regarding how a COMPAS assessment’s risk factors correlate with race”.<sup>51</sup>

In the end, though, Justice Bradley allowed sentencing judges to use COMPAS. However, she warned that judges must proceed with caution when using such risk assessments. They must take account of the algorithm’s limitations and the secrecy surrounding it, but said the software could be helpful, “in providing the sentencing court with as much information as possible in order to arrive at an individualized sentence”.<sup>52</sup>

To ensure that judges weigh risk assessments appropriately, the court advised both how these assessments must be presented to trial courts and the extent to which judges may use them. The court explained that risk scores may not be used, “to determine whether an offender is incarcerated”; or, “to determine the

---

<sup>50</sup> *State v. Loomis*, *supra* note 41 at 63.

<sup>51</sup> *Ibid.*

<sup>52</sup> *Ibid* at 72.

severity of the sentence.”<sup>53</sup> Therefore, judges using risk assessments must explain the factors other than the assessment that support the sentence imposed.

Furthermore, presentence investigation reports that incorporate a COMPAS assessment must include five written warnings for judges: first, the “proprietary nature of COMPAS” prevents the disclosure of how risk scores are calculated; second, COMPAS scores are unable to identify specific high-risk individuals because these scores rely on group data; third, although COMPAS relies on a national data sample, there has been “no cross-validation study for a Wisconsin population”; fourth, studies “have raised questions about whether [COMPAS scores] disproportionately classify minority offenders as having a higher risk of recidivism”; and fifth, COMPAS was developed specifically to assist the Department of Corrections in making *post*-sentencing determinations.<sup>54</sup> In issuing these warnings, the court made clear its desire to cast doubt upon the tool’s accuracy and reliability.

## CONCLUSION

The use of big data has already become a routine aspect of policing. These tools have clear benefits, including providing insights about how to direct police resources efficiently and effectively in ways that traditional policing methods have not been able to deliver. Digital policing helps reduce the criminal justice system’s overall burden, creating economies of scale in law enforcement and allowing police departments to maximize their limited resources.<sup>55</sup> One consequence is that digital policing will usually require offenders to expend more resources to plan, execute, and cover-up their crimes; and, this can lead to increased deterrence of some offenders as well as a greater number of crimes interrupted by the police before the offender can complete them.<sup>56</sup>

At the same time, this reliance upon artificial intelligence and the collection of vast amounts of information poses challenges for law enforcement and the courts. Digital policing creates a number of well-known concerns and it can also increase the privacy and civil liberties intrusions borne by law-abiding citizens. It can lead the police to focus on detecting crimes committed by certain populations and in certain locations, giving rise to concerns about racial and class bias. Furthermore, without adequate legal safeguards, once this data is collected and stored in bulk, it can be shared among various entities, including state and local law enforcement, the federal government, private contractors, civilian agencies, and the intelligence and military communities.<sup>57</sup>

---

<sup>53</sup> *Ibid* at 17.

<sup>54</sup> *Ibid* at 100.

<sup>55</sup> Manuel A. Utset, “Digital Surveillance and Preventive Policing” (2017) 49 Conn. L. Rev. 1453 at 1456.

<sup>56</sup> *Ibid* at 1474.

<sup>57</sup> Hu, *supra* note 6 at 1444.