# The Ubiquity and Risk of Algorithms

Mary W. Gray[1]
[1]American University, 4400 Massachusetts Avenue NW, Washington DC 20016

**Abstract**
Algorithms are determining who is arrested and the sentencing of those convicted, as well as decisions on medical care, school admission, insurance, employment, housing, voting,, and other essentials of life today. If the algorithm is patented or classified as proprietary, there may be little recourse by the subject or her/his attorneys should impermissible factors be used in constructing the decision-determining algorithms. This is becoming of increasing concern today because of the wide-spread use of machine-learning to construct complex, multiple versions of algorithms tailored to produce results that may cause physical or mental harm to individuals throughout the world as well as constituting substantial invasions of privacy. Examples from human rights, national and international law, economic development, journalism and government actions will be discussed.

**Key Words:** machine learning, intellectual property, product liability

## 1. Who Gets Out of Prison, Who Gets to Die?

Does being male qualify one as "high risk" and thus subject to a longer sentence? Eric Loomis thought so when he challenged the use of the algorithm COMPAS to determine the length of his sentence. Alas, he was not to know whether it was that characteristic or some other attribute, constitutionally prohibited or not, that led to the result. The U.S. Supreme Court refused to review the decision of the Wisconsin Supreme Court that had held the use of the algorithm to be permissible.. COMPAS, developed by the for-profit Northpointe, continues to be used by courts and parole boards around the country.

Glen Rodriquez was convicted of second-degree murder for his role at age 16 in an armed robbery resulting in a death. Although he had an exemplary record of rehabilitation in twenty-six years of prison and a job assured on his release, he was denied parole after COMPAS classified him as "high risk." Neither he nor the parole board knew why since Northpointe claimed that their algorithm was a trade secret. Eventually Rodriguez was able to discover that the wrong box had been checked on the form used by Northpointe. Although the error was never corrected, a parole board finally overruled COMPAS, a rare result.

And then there was TrueAllele, the probabilistic genotyping software. Michael Robinson tried unsuccessfully to subpoena the source code in order to challenge its DNA determination that placed him near the scene of a double murder. In 2016 President Obama's Council on Science and Technology had found that more testing was needed to establish the validity of programs like TrueAllele. But the judge in Robinson's case denied his request because the developer of the code said that disclosure would allow others to copy the code and put him out of business.

So far there is no evidence that a sentence of death resulted explicitly from an algorithm. However the factors determining that such an outcome is permissible, as established through court rulings over the years, are complex and certainly difficult to understand and indeed to foresee. Perhaps retired Justice Harry Blackmun saw algorithms in the process when declaring: "I shall no long tinker with the machinery of death."

More broadly, the development of algorithms that predict "hot spots" for intensified policing may, if known, presents an invitation for the criminal activity to move elsewhere, where protection is sparse.

## 2. Protection of Intellectual Property

The treatment of the intellectual property protection of software has had a rocky history. The U.S. Constitution gives Congress the power:

***To promote the progress of science and useful arts, by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries.***

Congress and the courts have sometimes treated algorithms as products of nature, along with DNA and mathematical equations, sometimes as "writings" and other times as useful "discoveries," at least when coupled with instruments of physical change or applications of business plans. But either as writings, protected by copyright, or discoveries, protected by patent, software has protection for a limited limit before going into the public domain.

On the other hand, software that constitutes a commercial product whose value lies in its being secret, can be deemed a "trade secret" so long as care is taken to maintain the secrecy. Protection of trade secrets continues until they are no longer secret. Thus the result is the cases described here and many others as well, Were the courts themselves as a government agency to develop such algorithms, they would, at least in theory, be open to inspection were they to infringe on the rights of individuals.

While it is clear that there may be good reasons for keeping algorithms secret such as selection for IRS audits and airport security screenings, excessive secrecy can let police, courts or other authorities evade accountability for illegal or unconstitutional methods. And aside from the government intrusions, open access in compiling and sharing algorithms would help understanding of how drugs work in order to avoid bad interactions. As we come to understand the fallout from the ubiquity of algorithms, solution may be sought. Judicial oversight? Perhaps court experts, but the rare appointment of court experts has not always been successful.

## 3. Machine Learning

Beyond the "known" algorithms we have the category of "unknowns." Because most machine-learning models can't offer reasons for their judgments, how do we know if they have misfired? By accident or triggered intentionally by clever adversarial attacks?