EFF and ACLU Tell Federal Court that Forensic Software Source Code Must Be Disclosed

Can secret software be used to generate key evidence against a criminal defendant? In an amicus filed ten days ago with the United States District Court of the Western District of Pennsylvania, EFF and the ACLU of Pennsylvania explain that secret forensic technology is inconsistent with criminal defendants' constitutional rights and the public's right to oversee the criminal trial process. Our amicus in the case of *United States v. Ellis* also explains why source code, and other aspects of forensic software programs used in a criminal prosecution, must be disclosed in order to ensure that innocent people do not end up behind bars, or worse—on death row.

The Constitution guarantees anyone accused of a crime due process and a fair trial. Embedded in those foundational ideals is the Sixth Amendment right to confront the evidence used against you. As the Supreme Court has recognized, the Confrontation Clause's central purpose was to ensure that evidence of a crime was reliable by subjecting it to rigorous testing and challenges. This means that defendants must be given enough information to allow them to examine and challenge the accuracy of evidence relied on by the government.

In addition, the public has a constitutional right of access to court proceedings. While this right is not absolute, it is clearly implicated here, where the government seeks to use secret software to generate evidence of criminal culpability.

In this case, Mr. Ellis was accused of violating a federal law prohibiting people who have been previously convicted of a felony from possessing a firearm (18 U.S.C. 922(g)(1)). The weapon had not been found in Mr. Ellis's possession, but was found in a car he was allegedly driving. Law enforcement officers retrieved a swab of DNA mixture from the gun, which they submitted for analysis by the police forensic lab. The lab results were inconclusive as to whether Mr. Ellis

could have contributed to the DNA in the mixture. The mixture sample was then sent to Cybergenetics, the owner of the probabilistic DNA software TrueAllele. Using TrueAllele, the company ran numerous variations of tests on the sample using different hypotheses to adjust the program settings, including alternative theories regarding the number of people whose DNA was in the mixture.

Prosecutors in the case seek to rely on the result of one particular analysis based on the assumption that four people contributed to the DNA sample from the gun. The results of this particular analysis suggest that Mr. Ellis's DNA was present on the gun. In response, Mr. Ellis's attorney requested the source code for TrueAllele, but the government refused to disclose it, arguing that the information is protected by trade secrets.

As EFF has previously pointed out, DNA analysis programs are not uniquely immune to errors and bugs, and criminal defendants cannot be forced to take anyone's word when it comes to the evidence used to imprison them. Independent examination of the source code of forensic software similar to TrueAllele has revealed mistakes and flaws that call into question the accuracy of these tools and their suitability for the criminal justice system. A defendant's Sixth Amendment right to confrontation requires that they are provided with the information necessary to challenge and expose any material defects in the purported evidence of their guilt. In an exceptional case, a court could issue a protective order limiting disclosure to the defense team, but the default must be disclosure.

Without disclosure, we, as the public, cannot have confidence in a verdict against Mr. Ellis.

19-cr-00369_amicus_brief_of_eff_and_aclu.pdf

RELATED CASES:

UNITED STATES V. ELLIS

CALIFORNIA V. JOHNSON