NO. 17-50062

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,

PLAINTIFF-APPELLEE,

V.

JOSEPH NGUYEN,

DEFENDANT-APPELLANT.

On Appeal From The United States District Court
for the Southern District of California
Case No. 3:13-cr-3447-MMA
Honorable Michael M. Anella, District Court Judge

BRIEF OF *AMICUS CURIAE* ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF DEFENDANT-APPELLANT'S PETITION FOR REHEARING EN BANC

Stephanie Lacambra
Kit Walsh
ELECTRONIC FRONTIER
FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Facsimile: (415) 436-9993
stephanie@eff.org

Counsel for Amicus Curiae
Electronic Frontier Foundation

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, *Amicus Curiae* Electronic Frontier Foundation states that it does not have a parent corporation and that no publicly held corporation owns 10% or more of its stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Rules

Constitutional Provisions

Other Authorities

Roger A. Grimes, *Five Reasons Why Software Bugs Still Plague Us* (July 8, 2014) CSO Online 6

Sonari Glinton, *How A Little Lab In West Virginia Caught Volkswagen's Big Cheat* (Sept. 24, 2015) NPR Morning Edition 7

STATEMENT OF INTEREST

The Electronic Frontier Foundation ("EFF") EFF is a San Francisco-based, donor-supported, non-profit civil liberties organization working to protect and promote fundamental liberties in the digital world. Through direct advocacy, impact litigation, and technological innovation, EFF's team of attorneys, activists, and technologists encourage and challenge industry, government, and courts to support free expression, privacy, and transparency in the information society. EFF has over 37,000 dues-paying members, over 400,000 subscribers, and represents the interests of everyday users of the Internet. EFF has special familiarity with and interest in constitutional privacy issues that arise with new technologies, and has served as amicus in recent key First and Fourth Amendment cases including *Carpenter v. U.S.*, (No. 16-402) 138 S.Ct. 2206 (2018) (seizure of historical cell site location information from a third party constitutes a search); *U.S. v. Robert McLamb*, (No. 17-4299) 880 F.3d 685 (4th Cir. 2018) (government hacking of digital devices); *Riley v. State of California*, (No. 13-132 & 13-212) 134 S.Ct 2473 (2014) (warrantless search of a cellphone); and *Mohamed v. Jesppesen Dataplan, Inc.*, (No. 08-15693) 614 F.3d 1070 (9th Cir. 2010) (decrying the government's use of the state secret privilege to bar justiciability).

Pursuant to Federal Rule of Appellate Procedure 29(c)(5), no one, except for undersigned counsel, has authored the brief in whole or in part, or contributed money towards the preparation of this brief. Neither party opposes the filing of this brief. Plaintiffs-Appellee defer to the court's decision on the filing of this brief and Defendant-Appellant consents to the filing of this brief.

POINTS AND AUTHORITIES

The Constitution requires that defendants be given the opportunity to review, analyze, and respond to the prosecution's evidence. Increasingly, prosecutors are relying on evidence produced by forensic software programs – marketed and distributed by private companies to law enforcement – to establish key elements of their case, while seeking to keep the source code that determines the outputs of that forensic technology a secret.

Ostensibly, the secrecy of forensic software source code is meant to prevent commercial misappropriation, but it also prevents defendants and the public from discovering flaws in the software that send innocent people to prison or execution. Time and again, when forensic software is subjected to independent review, errors and inconsistencies are discovered that call into question its viability and suitability for use in the criminal justice system.

Where the government seeks to use evidence generated by forensic software owned by a private third party, disclosure of the software's source code is required by the Constitution and by the strong public interest in the integrity of court proceedings. At most, the proponent of a trade secret may seek to establish that a protective order is necessary so that only the defendant's attorneys and retained experts get access to the source code. Protective orders are commonly used where the stakes are much lower, as in a commercial dispute, and the chance of misappropriation is higher because the parties are direct competitors. In the context of a criminal prosecution, where the public has a compelling interest in the Constitutional guarantees of a fair and public trial, public disclosure is all the more appropriate and should be the rule, with the prosecution bearing the burden to prove that an exception is justified.

I. Due Process Requires Disclosure of Source Code Relied Upon by the Prosecution

U.S. criminal court proceedings are presumptively open to the public under both Supreme Court precedent and our common law tradition.[1] The Bill of Rights goes even further to guarantee an accused the right to review and meaningfully confront the prosecution's evidence, and prohibits the prosecution from shifting its burden of proof to the defense.[2] Accordingly, disclosure of evidence relied upon by the prosecution – even privately owned forensic software source code – is mandated by both our Constitution and common law.

[1] *Richmond Newspapers, Inc. v. Virginia*, 448 U.S. 555, 580, n.17 (1980) (upholding presumption that criminal trials be open to the public and recognizing the common-law tradition "that historically both civil and criminal trials have been presumptively open.").

[2] U.S. Const., amend. VI, amend. XIV.

A. Due Process Entitles the Defense to Review the Prosecution's Evidence

Defendants have both a Constitutional and statutory right to receive and review the evidence against them. Evidence must be produced to the defense pursuant to both the Fourteenth Amendment guarantee of due process and the Sixth Amendment rights to a fair trial and to "be informed of the nature and cause of the accusation; to be confronted with the witnesses against him; [and] to have compulsory process for obtaining witnesses in his favor."[3]

Federal Rule of Criminal Procedure 16 (a)(1) specifically provides for the production of "(E) Documents and Objects"; and "(F) Reports of Examinations and Tests."[4]

[3] *Id.*

[4] Federal Rule of Criminal Procedure 16 (a)(1)
(E) Documents and Objects. Upon a defendant's request, the government must permit the defendant to inspect and to copy or photograph books, papers, documents, data, photographs, tangible objects, buildings or places, or copies or portions of any of these items, if the item is within the government's possession, custody, or control and:
(i) the item is material to preparing the defense;
(ii) the government intends to use the item in its case-in-chief at trial; or
(iii) the item was obtained from or belongs to the defendant.
(F) Reports of Examinations and Tests. Upon a defendant's request, the government must permit a defendant to inspect and to copy or photograph the results or reports of any physical or mental examination and of any scientific test or experiment if:
(i) the item is within the government's possession, custody, or control;
(ii) the attorney for the government knows--or through due diligence could know--that the item exists; and

There is no justification for subjugating these Constitutional and statutory rights to private business interests in maintaining a purported trade secret. Defendants are entitled to review the source code upon which the prosecution's case relies.

B. Defense Review of Source Code Used by the Prosecution to Establish Guilt is Essential to the Fair Resolution of a Criminal Proceeding

When hidden software code produces the prosecution's key forensic evidence of guilt or forms the basis for the issuance of a search warrant, the defendant's fate can be determined by a black box that the defense has no opportunity to examine or challenge. Software errors are common and forensic software has no special immunity from the bugs and mistakes that plague software in other fields. The defense must be allowed to review the source code and developmental materials in order to understand and meaningfully confront the prosecution's assertion that a single IP address was identified as storing and housing a complete file of suspected child pornography – an element essential to the prosecution's case.

(iii) the item is material to preparing the defense or the government intends to use the item in its case-in-chief at trial.

1. *It is routine to discover flaws in software via adversarial and independent analysis.*

Software errors are extremely common. While most mistakes in software are caught before products are released, many are not and these bugs cost the economy billions of dollars every year.[5] As software becomes ever more complex, and interacts with increasingly complex systems, errors become harder to prevent.[6] Some bugs are fairly easy to discover, as when a bug causes a program to crash. But for other errors, the software will appear to function properly but will output incorrect results. Such errors often go undiscovered for years.

To take a famous and venerable example, the hole in the ozone layer went undiscovered for years because NASA's software was programmed to ignore outlier data that the original programmers had assumed was unrealistic.[7] A recent software error in Ireland's National Integrated Medical Imaging System "meant potentially thousands of patient records from MRIs, X-rays, CT scans and

[5] *See* Michael Zhivich & Robert K. Cunningham, *The Real Cost of Software Errors* (Mar. 1, 2009) IEEE Security & Privacy, at https://dspace.mit.edu/openaccess-disseminate/1721.1/74607.

[6] Roger A. Grimes, *Five Reasons Why Software Bugs Still Plague Us* (July 8, 2014), CSO Online at https://www.csoonline.com/article/2608330/security/5-reasons-why-software-bugs-still-plague-us.html.

[7] Michael King and David Herring (Dec. 10, 2001) *Research Satellites for Atmospheric Sciences, 1978-Present, Serendipity and Stratospheric Ozone*, NASA's Earth Observatory at https://earthobservatory.nasa.gov/Features/RemoteSensingAtmosphere/remote_sensing5.php.

ultrasounds were recorded incorrectly."[8] The error involved a misplaced less-than (<) symbol and may have led to thousands of unnecessary medical procedures. A large Australian bank recently admitted a software error had caused it to fail to report certain transactions for almost three years, leading to widespread money laundering.[9] In rare cases, software errors may even be introduced intentionally, as was the case with Volkswagen software designed to make its vehicles produce inaccurate emissions readings during testing.[10] Of course, the vast majority of software errors are mere oversights, but that does not make their impact any less serious.

Forensic technology is not immune to software errors.[11] Indeed, as such technology becomes more complex it is at risk of error just like all complex software. Independent public scrutiny and testing is the best way to discover such

[8] Jack Power, *Software company behind HSE scan glitch begins investigation* (Aug. 5, 2017) The Irish Times at https://www.irishtimes.com/news/ireland/irish-news/software-company-behind-hse-scan-glitch-begins-investigation-1.3178349.

[9] Allie Coyne*, CBA blames coding error for alleged money laundering* (Aug. 7, 2017) itnews at https://www.itnews.com.au/news/cba-blames-coding-error-for-alleged-money-laundering-470233.

[10] Sonari Glinton, *How A Little Lab In West Virginia Caught Volkswagen's Big Cheat* (Sept. 24, 2015) NPR Morning Edition at http://www.npr.org/2015/09/24/443053672/how-a-little-lab-in-west-virginia-caught-volkswagens-big-cheat.

[11] Andrea Roth, *Machine Testimony*, 126 Yale L. J. 1972, 1983-93 (May 2017); Christian Chessman, *A 'Source' of Error: Computer Code, Criminal Defendants, and the Constitution*, 105 Cal. L. Rev. 179 (Feb. 2017).

errors.[12]

For example, the President's Council of Advisors on Science and Technology (PCAST) issued a report emphasizing the need for independent review of probabilistic DNA programs used in criminal prosecutions, in part to determine "whether the software correctly implements the methods" on which the analysis is based.[13]

The worst-case scenario is that secret, unverified code is contributing to the conviction of innocent people, and that is exactly what researchers discovered when they were finally able to review the source code of DNA software used in New York crime labs. When FST – a probabilistic DNA software program – was finally disclosed for analysis, the defense expert discovered a previously-undisclosed portion of the code that incorrectly tipped the scales in the prosecution's favor.[14] They also determined that the code actually used in crime labs was not even the same as the code sent for peer review.[15] Likewise, when

[12] *See* Edward J. Imwinkelried, Computer Source Code: *A Source of the Growing Controversy Over the Reliability of Automated Forensic Techniques*, 66 DePaul L. Rev. 97 (Fall 2016) .

[13] President's Council of Advisors on Science and Technology (PCAST), *Report to the President: Forensic Science in Criminal Courts: Ensuring Scientific Validity of Feature-Comparison Methods* (Sept. 2016) p. 79, at https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_forensic_science_report_final.pdf.

[14] *United States v. Kevin Johnson,* 15-CR-565 (VEC) (S.D.N.Y. Feb. 27 2017), D.I. 110 at pp. 17-19.

[15] *Id.*

STRMix (a similar tool) was analyzed by independent researchers, they found programming errors that created false results in 60 out of 4500 cases in Queensland, Australia.[16] The basic requirement of independent testing applies not only to DNA analysis tools, but also to other computerized forensic software such as the software that runs breathalyzers.[17] Courts have ordered the disclosure of such source code, as well as independent testing, and experts have found errors even in the relatively simple software involved in breathalyzer tests.[18]

The only way to be certain that biased datasets, assumptions, or functions are not distorting a forensic program's outputs, and to understand precisely how a technology controls for them, is to examine the source code and developmental materials.

[16] David Murray, *Queensland authorities confirm 'miscode' affects DNA evidence in criminal cases* (Mar. 20, 2015) Courier Mail, at http://www.couriermail.com.au/news/queensland/queensland-authorities-confirm-miscode-affects-dna-evidence-in-criminal-cases/news-story/833c580d3f1c59039efd1a2ef55af92b.

[17] *State v. Chun*, 194 N.J. 54, 127 (N.J. 2008) (error in one version of breathalyzer code resulted in incorrect results); *see State v. Underdahl*, 767 N.W.2d 677 (Minn. 2009) (potential defects that could be detected in breathalyzer source code warranted order to disclose complete source code); *see also Davenport v. State*, 289 Ga. 399, 404 (Ga. 2011) (Nahmias, J., *concurring*) (noting potential due process concerns if source code for forensic machines could not be discovered, lauding majority decision for rejecting such a conclusion and remanding).

[18] *Id.*

2. *Given the potential for error and undisclosed assumptions, source code and developmental material review is essential to a fair resolution.*

Given the foregoing, meaningful confrontation of the secret software program used by law enforcement to isolate and connect to a computer associated with a specific IP address and to allegedly download a video file in its entirety[19], necessarily depends on the defense's access to and opportunity to review the source code, developmental materials, and the assumptions embedded within them. They must therefore be disclosed.

Failure to disclose the source code and developmental materials would work an injustice that fundamentally undermines the adversarial process in that one side (the prosecution) would have use of evidence reasonably believed to be essential to a fair resolution of the lawsuit – namely, the program methodology that must be examined for accuracy, functionality and credibility in order to meaningfully confront the forensic program's results – which was denied to the opposing party. If the software does not, in fact, correctly download the file from only one potential source while blocking the others, then it could yield false results, downloading the file from multiple sources while reporting that a single source provided the file in its entirety.

[19] ER:25-26.

Without disclosure and review, the prosecution is simply asking defendants and the public to take their word for it; that is not the way the criminal justice system works in a nation with guarantees of due process, confrontation, and the fair and open administration of justice.

3. Exclusion is the appropriate remedy for non-disclosure.

Where the prosecution refuses to disclose evidence upon which it relies, exclusion is the only appropriate remedy. Our justice system cannot contemplate convictions based on secret evidence.[20] To do so would pervert the equitable principles upon which our common law right to access criminal proceedings[21] and our Constitutional guarantee of due process[22] were founded.

The Minnesota Supreme Court agrees, reasoning that prejudicial failure to disclose information such as forensic methodology on the basis that the method was a trade secret provided grounds for excluding the evidence because "access to the data, methodology, and actual results is crucial so a defendant has at least an

[20] *See* U.S. Const. amend. VI ("In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial…and to be informed of the nature and cause of the accusation; to be confronted with the witnesses against him; to have compulsory process for obtaining witnesses in his favor,"); *Richmond Newspapers*, 448 U.S. at 580 (First amendment requires criminal trials be open to the public).

[21] *Richmond Newspapers*, 448 U.S. at 580, n.17 (recognizing the common-law tradition "that historically both civil and criminal trials have been presumptively open.").

[22] U.S. Const. amend. XIV.

opportunity for independent expert review."[23]

C. Due Process Prohibits Burden Shifting to the Defense

The Fourteenth Amendment safeguards individual rights to due process of law, which dictate that "a State must prove every ingredient of an offense beyond a reasonable doubt, and . . . may not shift the burden of proof to the defendant . . . ."[24] By the same token, "a presumption which, although not conclusive, had the effect of shifting the burden of persuasion to the defendant," is unconstitutional.[25] Thus, any framework that imposes an evidentiary burden upon defense as a prerequisite to obtaining access to evidence that forms the basis of the criminal prosecution both contorts and contravenes basic Constitutional guarantees and cannot withstand scrutiny. Such a framework impermissibly shifts the burden of persuasion to defense to show that the evidence that forms the backbone of the prosecution's forensic case is relevant to the defense theory, and to do so without having the opportunity to examine the evidence in the first place. It's akin to asking a mechanic to certify a car is in good working condition without allowing them to look under the hood. There are many things that could affect or influence the car's drivability, but they won't know until they inspect it. Because denying defense access to core forensic tools used by the prosecution fails to protect basic

[23] *State v. Schwartz,* 447 N.W.2d 422, 427-28 (Minn. 1989).
[24] *Patterson v. NY,* 432 U.S. 197, 215 (1977).
[25] *Sandstrom v. Montana,* 442 U.S. 510, 524 (1979); *see generally*, *Mullaney v. Wilbur,* 421 U.S. 684 (1975).

Constitutional guarantees, this Court should firmly reject such a framework.

II. In the Unusual Situation Where a Third Party's Interest Is Proven to Outweigh the Public's Compelling Interest in a Fair and Public Trial, A Protective Order Sufficiently Protects Trade Secrets in the Criminal Justice Context

The public's compelling interest in a fair and public trial should generally outweigh any third party's proprietary interest in hiding their purported trade secret. However, where a third party can prove that their monetary interest outweighs the public's interest in public access and oversight of judicial proceedings, courts may easily resolve any tension between the two with a simple protective order. But non-disclosure to the public should be the exception and not the rule.

It is common in civil cases to disclose trade secrets subject to protective orders, even to attorneys and experts representing competitors. It is so routine, in fact, that the federal district court for the Northern District of California has adopted a model protective order that specifically contemplates the disclosure of trade secrets and source code to opposing counsel and experts retained by the party, provided they agree to be bound by the order.[26]

Thus, disclosure subject to a protective order is routinely required when relevant.[27] This is so even when the parties are direct competitors with an interest

[26] *See* http://www.cand.uscourts.gov/model-protective-orders.

[27] *See*, *e.g.*, *Fed. Open Mkt. Comm. of Fed. Reserve Sys. v. Merrill,* 443 U.S. 340, 362, n.24 (1979) (noting how rare it is to bar disclosure); *see also*, Dustin B.

in profiting from proprietary information of the other.[28]

Yet prosecutors often urge courts to divert from established practice and deprive criminal defendants of access to forensic software relied upon by the prosecution – even subject to a protective order.

This proposed higher barrier to discovery is backwards. It should be *easier* for a defendant trying to defend their life and liberty to access relevant information, as compared to a party with a mere economic interest. Additionally, the public has an overriding interest in ensuring the fair administration of justice, which favors disclosure.[29]

It is particularly equitable to require the disclosure of trade secrets relating to forensic technology deployed in the criminal justice system, because any business entering the market should foresee that any secrecy it may seek to maintain will conflict with the strong public interest in the judicial system's transparency and reliability, as well as defendants' rights of confrontation and due process.

Moreover, trade secrecy is not the only business strategy that a forensic software company may employ. It could alternatively rely on other legal regimes or generate positive publicity through independent testing of non-secret software. A company's choice of one business model over another cannot overcome either

Benham, *Proportionality, Pretrial Confidentiality, and Discovery Sharing*, 71 Wash. & Lee L. Rev. 2181, 2240-2241 (2014).

[28] Benham, 71 Wash. & Lee L. Rev. at 2240-2241.

[29] *Richmond Newspapers*, 448 US at 580.

the public interest in transparent and fair justice, or a defendant's due process rights.

CONCLUSION

For the foregoing reasons, *amicus* respectfully requests this Court reverse and remand for the trial court to order disclosure of the source code and developmental program materials to defense or require exclusion of the evidence derived from the secret software program used by law enforcement in its entirety for the government's failure to disclose.

Dated: October 1, 2018

Respectfully submitted,

By: */s/ Stephanie Lacambra*

Stephanie Lacambra
Kit Walsh
ELECTRONIC FRONTIER
FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Facsimile: (415) 436-9993
stephanie@eff.org

Counsel for Amicus Curiae

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMITATION, TYPEFACE REQUIREMENTS AND TYPE STYLE REQUIREMENTS PURSUANT TO FED. R. APP. P. 32(A)(7)(C)

Pursuant to Fed. R. App. P. 32(a)(7)(C), I certify as follows:

1. This Brief of Amicus Curiae In Support of Defendants-Appellants' Petition For Rehearing En Banc complies with the length limits of Circuit Rule 29-2(c)(2) because this brief contains 3,287 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii); and

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2011, the word processing system used to prepare the brief, in 14 point, Times New Roman font.

Dated: October 1, 2018

By: *[/s/ Stephanie Lacambra]*
Stephanie Lacambra

Counsel for Amicus Curiae
ELECTRONIC FRONTIER
FOUNDATION

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on October 1, 2018.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

Dated: October 1, 2018

By: */s/ Stephanie Lacambra*
Stephanie Lacambra

Counsel for Amicus Curiae
ELECTRONIC FRONTIER
FOUNDATION