Case No. F071640

IN THE COURT OF APPEAL FOR THE STATE OF CALIFORNIA
FIFTH APPELLATE DISTRICT

THE PEOPLE OF THE STATE OF CALIFORNIA,

Plaintiff and Respondent,

v.

BILLY RAY JOHNSON, JR.,

Defendant and Appellant.

Appeal from the Superior Court for the State of California,
Kern County, Trial Case No. BF 151825 A
Hon. Gary T. Friedman

AMICUS CURIAE BRIEF OF ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF DEFENDANT AND APPELLANT BILLY RAY JOHNSON

Stephanie Lacambra (SBN 232517)
stephanie@eff.org
Kit Walsh (SBN 303598)
kit@eff.org
ELECTRONIC FRONTIER
FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Facsimile: (415) 436-9993

Counsel for Amicus Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Constitutional Provisions

ISSUE PRESENTED

Whether a defendant's due process rights to a fair and public trial outweigh a private business's commercial interest in preventing potential misappropriation of a purported trade secret in the functioning of forensic software used to inculpate the defendant.

INTEREST OF THE AMICUS CURIAE

The Electronic Frontier Foundation ("EFF") is a member-supported, non-profit civil liberties organization that has worked to protect free speech and privacy rights in the online and digital world for 27 years. With roughly 38,000 active donors, EFF represents the interests of technology users in court cases and broader policy debates surrounding the application of law in the digital age. 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 *ACLU of Southern California v. County of Los Angeles* (Cal. Aug. 31, 2017); __Cal.3d__ 2017 WL 3754336, 17 Cal. Daily Op. Serv. 8551; *Mohamed v. Jesppesen Dataplan, Inc.* (9th Cir. 2010) 614 F.3d 1070; and *Restis v. American Coalition Against Nuclear Iran, Inc.* (S.D.N.Y. 2014) 2014 WL 5369342.

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 a crime, 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. This includes counterparts to TrueAllele such as FST and STRMix, both of which have manifested serious errors that could be used to inculpate innocent people.

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. However, 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, not the exception.

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 enshrined in our Constitution 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.

A. Due Process Entitles 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 right 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]

California Penal Code section 1054.1 specifically provides for the production of "(c) All relevant real evidence seized or obtained as a part of the investigation of the offenses charged"; and "(f) Relevant written or recorded statements of witnesses or reports of the statements of witnesses…, including any reports or statements of experts made in conjunction with the

---

[1] *Richmond Newspapers, Inc. v. Virginia* (1980) 448 US 555, 580, n. 17 (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.

[3] *Id*.

case, including the results of physical or mental examinations, scientific tests, experiments, or comparisons."[4]

There is no justification for subjugating these Constitutional and statutory rights to private business interests in maintaining a purported trade secret. Defendants are thus 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, 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 in order to understand and meaningfully confront the prosecution's forensic evidence regarding the identity of the perpetrator – an essential element of the prosecution's case.

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

[4] Cal. Penal Code §1054.1

[5] *See* Michael Zhivich & Robert K. Cunningham, *The Real Cost of Software Errors* (Mar. 1, 2009) IEEE Security & Privacy, at https://ll.mit.edu/mission/cybersec/publications/publication-files/full_papers/2009_03_01_Zhivich_IEEES-P_FP.pdf

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 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

---

[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

[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

its vehicles produce inaccurate emissions readings during testing.[10] Of course, the vast majority of software errors are merely 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 (as with the new generation of DNA tools) it is at risk of error just like all complex software. Independent public scrutiny and testing is the best way to discover such errors.[12]

2. Probabilistic DNA tools embody a variety of potentially flawed assumptions and warrant rigorous independent testing.

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

For instance, when FST – a counterpart to TrueAllele used in New York crime labs – was finally disclosed for analysis, experts discovered a previously undisclosed portion of the code that incorrectly tipped the scales

---

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

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

[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. 78, at https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_forensic_science_report_final.pdf.

in favor of the prosecution's hypothesis that a defendant's DNA was present in a mixture.[14] They also determined that the code actually used in crime labs was not the same as the code sent for peer review.[15]

Likewise, when STRMix (another tool comparable to TrueAllele) 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 devices like breathalyzers, which utilize a more established scientific approach.[17]

However, the problems caused by nondisclosure are especially acute in the context of the latest generation of probabilistic DNA analysis because there is no objective baseline truth against which they may be evaluated. In the breathalyzer context, it's possible to evaluate the parts per million of alcohol in the air and the conclusion is an objective fact that can be compared against existing measurement technologies.

Not so with the latest generation of DNA analysis tools. These tools take in a sample that is thought to have DNA from multiple sources (such

---

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

[15] *Id.*

[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* (2008) 194 N.J. 54, 127 (error in one version of breathalyzer code resulted in incorrect results); *see State v. Underdahl* (Minn. 2009) 767 N.W.2d 677 (potential defects that could be detected in breathalyzer source code warranted order to disclose complete source code); *see also Davenport v. State* (2011) 289 Ga. 399, 404 (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).

as a swab from a handbag or weapon).[18] The device then analyzes the sample according to the assumptions programmed into it.

Because the output of newer DNA analysis tools depends on speculative assumptions,[19] different products like STRMix and TrueAllele provide drastically different estimates from one another – a discrepancy that can mean the difference between exculpation and inculpation.[20] As a result, these programmed assumptions, and the way they are coded into the software, are critical to the defense's ability to identify areas for challenges to its reliability and accuracy.

For instance, common random effects can alter DNA test results, and DNA analysis tools take different approaches to counteracting these effects or may fail to do so.[21] Two of these random phenomena are "allelic drop-in" and "allelic drop-out," which simply refer to the rate at which the technology loses track of existing DNA patterns (alleles) or falsely reports

---

[18] *See People v. Collins* (Kings Co. Sup. Ct. 2015) 49 Misc.3d 595, 613-616.

[19] *See*, *e.g.*, Paolo Garofano, et. al., *An Alternative Application of the Consensus Method to DNA Typing Interpretation for Low Template-DNA Mixtures* (2015) Forensic Sci. Int'l: Genetics Supp. Series 5, p.e422–e424.

[20] PCAST *Report to the President: Forensic Science in Criminal Court*, p.79, n. 212. *See e.g.*, *People v. Hillary,* Court No. 2015-15 (N.Y. Sup.Ct. St. Lawrence Co. 2016), at http://www.northcountrypublicradio.org/assets/files/08-26-16DecisionandOrder-DNAAnalysisAdmissibility.pdf; *see* Jesse McKinley, *Oral Nicholas Hillary Acquitted in Potsdam Boy's Killing* (Sept. 28, 2016) N.Y. Times at http://www.nytimes.com/2016/09/29/nyregion/oral-nicholas-hillary-potsdam-murder-trial-garrett-phillips.html; *see also*, PCAST, *An Addendum to the PCAST Report*, p.8, at https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_forensics_addendum_finalv2.pdf; P. Garofano et al., *An alternative application of the consensus method to DNA typing interpretation for Low Template-DNA mixtures* (2015) Forensic Sci. Int'l: Genetics Supp. Series 5 e422–e424.

[21] *See Collins,* 49 Misc.3d at 600, 604-606 (discussing stochastic effects in context of analyzing admissibility of probabilistic genotyping program).

their presence in a mixture.[22] The other common phenomena are more complicated, referred to as "exaggerated stutter" and "peak height imbalance," and these create the appearance of alleles that are in fact absent, or make it falsely seem that an allele is far more prevalent than others.[23] The only way to be certain that these effects are accounted for, and to understand precisely how a technology accounts for them, is to examine the source code.

3. Given those potential variations and assumptions, source code review is essential to a fair resolution.

Given the foregoing, meaningful confrontation of the True Allele program test results necessarily depends on the defense's access to and opportunity to review the source code and the assumptions embedded within it. It must therefore be disclosed.

By contrast, failure to disclose the True Allele source code would "work an injustice" within the meaning of California Evidence Code section 1060. 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 test results – which was denied to the opposing party.[24]

---

[22] *Id.* at 605-606.

[23] *Id.* at 606-610.

[24] *See Bridgestone/Firestone Inc. v. Sup. Ct.* (1992) 7 Cal.App.4th 1384, 1393 (finding that a court is required to order disclosure of a trade secret unless, after balancing the interests of both sides, it concludes that under the particular circumstances of the case, no fraud or injustice would result from denying disclosure); *Agricultural Labor Relations Bd.* (*ALRB*) *v. Richard A. Glass Co.* (1985) 175 Cal.App.3d 703 (held that allowing the trade secret privilege to stand would tend to work an injustice on the agricultural workers involved).

4. 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.[25] To do so would pervert the equitable principles upon which our common law right to access criminal proceedings[26] and our Constitutional guarantee of due process[27] were founded.

The Minnesota Supreme Court agrees. Addressing the issue in a similar context, the court reasoned 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 opportunity for independent expert review."[28]

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 . . . ."[29] By the same token, "a presumption which, although not conclusive, had the effect of shifting the burden of persuasion

---

[25] *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).

[26] *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.")

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

[28] *State v. Schwartz* (Minn. 1989) 447 N.W.2d 422, 427-28.

[29] *Patterson v. NY* (1977) 432 U.S. 197, 215.

to the defendant," is unconstitutional.[30] 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.

This much would seem incontrovertible. However, in an unpublished/nonciteable opinion, the second district of the Court of Appeal of California, Division 4, erroneously held that a defendant in a criminal case cannot review material alleged to be a trade secret unless they can show that such access is "relevant and necessary to the proof, or defense against, a material element of one or more causes of action presented in the case, and that it is reasonable to conclude that the information sought is essential to a fair resolution of the lawsuit"[31] before evidentiary access is granted.

The *Chubbs* court's flawed reasoning should not influence this Court. It 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 as 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 this framework fails to protect basic Constitutional guarantees, this Court should firmly reject it.

---

[30] *Sandstrom v. Montana* (1979) 442 U.S. 510, 524; *see generally*, *Mullaney v. Wilbur* (1975) 421 U.S. 684.

[31] *See People v. Superior Court (Chubbs)* (2015) (not published) 2015 WL 139069 at *5.

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, the Court 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.

A. Common Practice and Equity Require Disclosure of Trade Secret Information Where, as here, it is Material to the Defense

As a general rule, where the prosecution seeks to withhold evidence by claiming a trade secret privilege, it must first carry the burden of showing that the evidence qualifies as a trade secret by filing a motion and accompanying affidavit by someone with personal knowledge qualified to give such an opinion.[32] If the prosecution meets that burden, courts still require disclosure, but impose a protective order.[33]

It is equally 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 who agree to be bound by the

---

[32] *See* Evid. Code § 1061(b)(1); *see Bridgestone/Firestone*, 7 Cal.App.4th at 1393 (held that the party claiming the privilege has the burden of establishing its existence).

[33] *See* Evid. Code § 1061(b)(4).

order.[34]

Thus, disclosure subject to a protective order is routinely required when relevant.[35] This is so even when the parties are direct competitors with an interest in profiting from proprietary information of the other.[36]

Yet prosecutors here urge the Court 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.[37]

It is particularly equitable to require the disclosure of trade secrets relating to forensic technology, 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 the public interest in transparent and fair justice, or a defendant's due process rights.

---

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

[35] *See*, *e.g.*, *Fed. Open Mkt. Comm. of Fed. Reserve Sys. v. Merrill* (1979) 443 U.S. 340, 362, n.24 (noting how rare it is to bar disclosure); *see also*, Dustin B. Benham, *Proportionality, Pretrial Confidentiality, and Discovery Sharing* (2014) 71 Wash. & Lee L. Rev. 2181, 2240-2241.

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

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

B. The Prosecution Has Not, and Generally Cannot, Establish that Disclosure Subject to a Protective Order Would Cause Harm

Where disclosure is sought pursuant to a protective order, the court must weigh the risk of harm from disclosure *subject to the protective order*, rather than presuming disclosure to the public.[38] It is very unlikely for harm to result from disclosure to attorneys and retained experts subject to a protective order.[39]

Disclosure to defense attorneys subject to a protective order is not cognizable harm under substantive trade secrets law. Therefore, there is no risk of harm from disclosing the source code in this case, and the trial court should have required its disclosure.

CONCLUSION

For the foregoing reasons, *amicus* respectfully requests this Court reverse and remand for the trial court to order disclosure of the True Allele source code to defense or require exclusion of the DNA test results for failure to disclose the source code.

Dated: September 13, 2017

Respectfully submitted,

/s/ Stephanie Lacambra

Stephanie Lacambra
stephanie@eff.org
Kit Walsh
kit@eff.org

[38] *Coca-Cola Bottling Co. of Shreveport v. Coca-Cola Co.* (D. Del. 1985) 107 F.R.D. 288, 293.

[39] *See United States v. United Fruit Co.* (5th Cir. 1969) 410 F.2d 553, 556 (cert denied) (disclosure is less likely when made to a party that is not a competitor).

ELECTRONIC FRONTIER
FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333

CERTIFICATE OF COMPLIANCE

I certify pursuant to California Rules of Court 8.204(c) that this Amicus Curiae Brief of Electronic Frontier Foundation is proportionally spaced, has a typeface of 13 points or less, contains 3,808 words, excluding the cover, the tables, the signature block, verification, and this certificate, which is less than the total number of words permitted by the Rules of Court. Counsel relies on the word count of the Microsoft Word word-processing program used to prepare this brief.

Dated: September 13, 2017

/s/ Stephanie Lacambra
Stephanie Lacambra

ELECTRONIC FRONTIER FOUNDATION

Counsel for Amici Curiae

CERTIFICATE OF SERVICE

The undersigned declares:

I am over the age of 18 years and not a party to the within action. My business address is 815 Eddy Street, San Francisco, California 94109.

On September 13, 2017, I caused to be served copies of the foregoing documents described as:

AMICUS CURIAE BRIEF OF ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF DEFENDANT-APPELLANT BILLY RAY JOHNSON, JR.

on the parties in this action as follows:

SEE ATTACHED SERVICE LIST

☑ BY TRUEFILING: I caused to be electronically filed the foregoing document with the court using the court's e-filing system. The following parties and/or counsel of record are designated for electronic service in this matter on the TrueFiling website.

☑ BY FIRST CLASS MAIL: I caused to be placed the envelope for collection and mailing following our ordinary business practices. I am readily familiar with this firm's practice for collecting and processing correspondence for mailing. On the same day that correspondence is placed for collection and mailing, it is deposited in the ordinary course of business with the United States Postal Service, in a sealed envelope with postage fully prepaid

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct and that this document was executed on September 13, 2017.

By: /s/ Stephanie Lacambra
Stephanie Lacambra

SERVICE LIST

Office of the Attorney General
P. O. Box 944255
Sacramento, CA 94244

Via E-File Service

Caely E. Fallini
Office of the Attorney General
P.O. Box 944255
Sacramento, CA 94244

Via E-File Service

Attorneys for Plaintiff and Respondent The People of California

Laura Schaefer
Attorney at Law
934 23rd St.
San Diego, CA 92102

Via E-File Service

Attorneys for Defendant and Appellant Billie Ray Johnson, Jr.

Gerald Bill Hrycyszyn
Wolf Greenfield & Sacks PC
600 Atlantic Avenue, Ste. 2300
Boston, MA 02210

Via E-File Service

Attorneys for Amici Curiae The Innocence Project, Inc., The California Innocence Project, The Northern California Innocence Project, and The Loyola Law School's Project For the Innocent

Central California Appellate Program
2150 River Plaza Dr., Ste. 300
Sacramento, CA 95833

Via First Class Mail

Judge Gary T. Friedman
Kern County Superior Court
Metropolitan Division, Dept. 3
1415 Truxtan Avenue
Bakersfield, CA 93301

Via First Class Mail