No. 18-50440

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA

Plaintiff-Appellee,

vs.

LUKE WILSON,

Defendant-Appellant.

On Appeal from the United States District Court
for the Southern District of California
Case No. 15-cr-2838
The Hon. Gonzalo P. Curiel, District Judge Presiding

BRIEF OF *AMICUS CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER (EPIC) IN SUPPORT OF APPELLANT

Marc Rotenberg
Counsel of Record
Alan Butler
Megan Iorio
Electronic Privacy Information Center
1718 Connecticut Avenue, N.W.
Suite 200
Washington, DC 20009
(202) 483-1140

March 28, 2019

CORPORATE DISCLOSURE STATEMENT

Pursuant to Fed. R. App. P. 26.1, 29(c), and Local Rule 26.1 *Amicus Curiae* Electronic Privacy Information Center ("EPIC") is a District of Columbia corporation with no parent corporation. No publicly held company owns 10% or more of EPIC stock. No publicly held company has a direct financial interest in the outcome of this litigation by reason of a franchise, lease, other profit sharing agreement, insurance, or indemnity agreement.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

INTEREST OF AMICUS

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other constitutional values.[1]

EPIC routinely participates as *amicus curiae* before the United States Supreme Court and other courts in cases concerning emerging privacy issues, new technologies, and constitutional interests. EPIC has authored several briefs specifically concerning Fourth Amendment standards for searches using new technologies. *See*, *e.g.*, Brief of *Amici Curiae* EPIC et. al, *Carpenter v. United States*, 138 S. Ct. 2206 (2018) (arguing that technological changes since the era of analog phones justify departing from the third party doctrine); Brief of *Amici Curiae* EPIC et. al, *Riley v. California*, 134 S. Ct. 2473 (2014) (arguing that the warrantless search of a cell phone incident to an arrest is impermissible); Brief of *Amicus Curiae* EPIC, *Florida v. Harris*, 133 S. Ct. 1050 (2013) (arguing that the Government bears the burden of establishing the reliability of techniques used in criminal investigations). Last year, EPIC filed an *amicus* brief in a Sixth Circuit case similar to the present case. *See* Brief of *Amicus Curiae* EPIC, *United States v.*

[1] The parties consent to the filing of this *amicus curiae* brief. In accordance with Fed. R. App. P. 29, the undersigned states that no monetary contributions were made for the preparation or submission of this brief, and this brief was not authored, in whole or in part, by counsel for a party.

Miller, No. 16-47, 2017 WL 2705963 (E.D. Ky. Jun. 23, 2017), *appeal docketed*, No. 18-5578 (6th Cir. Jun. 5, 2018).

SUMMARY OF ARGUMENT

This case concerns Google's use of a proprietary algorithm to routinely scan the personal files of billions of Internet users for content that the company deems unlawful to possess. If the secret matching criteria that Google has developed are triggered, Google sends personal information about the user who uploaded the file to a law enforcement agency for criminal investigation. Google and the Government have both downplayed the risk of false positives as well as the subjective determinations that provide the basis for finding that certain content is unlawful to posses. They have not made the algorithm available for inspection or established that it can reliably identify files as containing contraband. Moreover, image matching techniques, at issue in this case, do not operate the same way as file hash functions, which do in fact confirm that two files are identical. And the law review article that the lower court in this case relied upon never made this distinction or discussed the use of image matching techniques.[2]

Cryptographic hash functions create a unique alphanumeric string, called a "hash value," associated with a digital file; that value can be used to "match" two files that are identical in every respect. In contrast, image matching techniques, like Microsoft's PhotoDNA, manipulate and analyze image data in order to determine whether *different* files contain the same image. An image matching technique can

[2] Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 Harv. L. Rev. 38, fn.a1 (2005).

enable a service provider such as Google to identify many different files that may contain the same or similar image, even if that image was altered, such as by cropping or resizing. But that capability also introduces the risk of false positives that do not exist in file hashing techniques.

Neither Google nor the Government has revealed the specific nature of the image matching technique at issue in this case. More critically, neither Google nor the Government has established the accuracy, reliability, or validity of the technique, which are fundamental requirements that courts require for scientific techniques in the law enforcement realm. Transparency is necessary because the consequences of an error are severe—automatic referral of a user's data, files, and identity to the National Center for Missing and Exploited Children ("NCMEC") and a subsequent investigation and referral to local law enforcement.

Algorithms that scan the internet for suspected contraband have far reaching consequences. Use of this technique for other purposes, e.g., to determine if files contain religious viewpoints, political opinions, or "banned books," would raise profound First Amendment concerns. Indeed, Google is currently facing criticism concerning Project DragonFly, a search engine designed for the Chinese government that enables the identification of materials that China would consider "politically sensitive." Brian Fung, *Google Really is Trying to Build a Censored*

Chinese Search Engine, Its CEO Confirms, Wash. Post (Oct. 16, 2018).[3] Even when the technique focuses on pornographic images, the risk is high that works of art, literature, and political commentary, will be caught in the algorithm's net. *See, e.g., Oklahoma ex rel. Macy v. Blockbuster Videos, Inc.*, No. 97-1281, 1998 WL 1108158 (W.D. Okla. Oct. 20, 1998) (finding that the Academy Award winning film *The Tin Drum* was not subject to Oklahoma's ban on child pornography).

The Fourth Amendment permits neither outcome. The private search doctrine does not allow the Government to obtain personal records from Internet companies without ensuring with "virtual certainty" that the Government otherwise has the authority to obtain the information sought.

ARGUMENT

As the Supreme Court recently recognized, "seismic shifts in digital technology" require a reexamination of existing Fourth Amendment standards. *Carpenter v. United Sates,* 138 S. Ct. 2206, 2219–20 (2018). The Court in *Carpenter* determined that the Fourth Amendment required a warrant for the automated search of cell cite location information. The Court recognized that individuals have both "a reasonable expectation of privacy in the whole of their physical movements," and that "law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every

[3] https://www.washingtonpost.com/technology/2018/10/16/google-really-is-trying-build-censored-chinese-search-engine-its-ceo-confirms/.

single movement of an individual's car for a very long period." *Id.* at 2217. Therefore, a Fourth Amendment rule permitting suspicionless tracking of suspects in the physical world where such tracking "for any extended period of time was difficult and costly and therefore rarely undertaken," *id.*, could not justify the vast capabilities of digital surveillance.

The same can be said about the private search doctrine as applied to the continuous scanning of private files, stored on computer servers across the country. Even if a court determines that this was a "private search" because Google did not act as a government agent in this case, the Fourth Amendment requires that any "additional invasions of respondents' privacy by the government agent must be tested by the degree to which they exceeded the scope of the private search." *United States v. Jacobsen*, 466 U.S. 109, 131 (1984). In *Jacobsen*, the Court held that the Government's warrantless inspection and testing of the contents of a package that had been previously searched by FedEx was permissible because "there was a virtual certainty" that the law enforcement officer's search would not reveal "anything more than he had already been told." *Id*. at 119.

This Court should recognize that a search is not reasonable under the private search doctrine if (1) the search relies on a private company's proprietary technique, (2) the technique is used routinely to search billions of files, and (3) the Government does not establish the reliability of the technique with a "virtual

certainty." Under the traditional private search doctrine, the Government would be prohibited from opening and inspecting files absent a showing that there was a "virtual certainty" that the same material had been previously searched by a private party. *United States v. Ackerman*, 831 F.3d 1292, 1305 (10th Cir. 2016) (Gorsuch, J.). And here the technique deployed by Google routinely searches millions of files and is not subject to independent inspection or verification. Moreover, the Government has not provided sufficient evidence in this case to establish with "virtually certainty" that the images sent in a CyberTipline Report to the NCMEC were the same as those uploaded by the user. Because Google's image matching technique does not function the same way as better-known file hashing techniques, and because neither Google nor the Government have explained how the image matching technique actually works or presented evidence establishing the algorithm's accuracy and reliability, the Government's search here was unreasonable.

I. Google's scanning technique implicates the privacy of more than a billion Internet users and there is a risk of false positives.

As part of the coordinated effort among electronic communications service providers, the NCMEC, and government investigators, Google scans billions of files to identify suspected contraband. *See* Declaration of Cathy McGoff ¶ 4, ECF No. 62-2, *United States v. Wilson*, No. 3:15-cr-2838, 2017 WL 2733879 (S.D. Cal. Jun. 26, 2017) (describing how Google compares "content uploaded to [their]

services" to the hashes of previously flagged images). Google submits reports of flagged images to NCMEC pursuant to 18 U.S.C. § 2258A(a)(2). The sheer volume of data subjected to these searches, including private files uploaded to cloud storage on the largest platforms, means that the risk of error in the identification or algorithmic matching of these images is significant. If a non-contraband image is added to one of these lists, or if a provider's algorithm falsely matches a non-contraband image with one of the records from its list, many innocent users could immediately have their confidential files and personal information relayed to law enforcement, and would be subject to an intrusive investigation as a result. Strong safeguards are needed to protect the interests of Internet users, especially because a false positive would not likely be subject to judicial review.

Recent studies confirm that e-mail is "the most pervasive form of communication." Radicati Group, Inc., *Email Statistics Report, 2018-2022: Executive Summary*, at *2 (2018).[4] In 2018, there were an estimated 3.8 billion e-mail users worldwide—and the number of accounts is growing at an even faster rate than the number of users. *Id*. at 3.[5] The largest email provider in the world is Google, with more than 1.5 billion Gmail users. @Gmail, Twitter (Oct. 26, 2018

[4] https://www.radicati.com/wp/wp-content/uploads/2018/01/Email_Statistics_Report,_2018-2022_Executive_Summary.pdf.
[5] The recent survey estimates an average 1.75 accounts per user, which is expected to grow steadily over the next four years. *Id*.

9:02 AM).[6] And e-mail only represents a small portion of Google's services. The company controls a wide range of internet services that enable users to upload images and other files. This includes Google Photos, Google Drive, Google Docs, and YouTube. *See* Google, *Our Products* (2019).[7] Google's file storage service, alone, had an estimated 1 billion users worldwide as of 2018. Shoshana Wodinsky, *Google Drive is About to Hit 1 Billion Users*, The Verge (Jul. 25, 2018).[8] This means that Google is scanning millions and millions of files each day.

Given the number of private files that are subject to Google's scanning algorithm, the potential impact of a false positive is significant and should be treated accordingly. The history of this case and other similar cases reveals the typical process that follows a positive match by Google's scanning algorithm. After an image is flagged, Google automatically submits a CyberTipline Report to NCMEC, which includes:

- the date and time of the incident;
- the e-mail address associated with the user account that uploaded the file;
- the IP address associated with the upload;

[6] https://twitter.com/gmail/status/1055806807174725633.
[7] https://www.google.com/about/products/. Even the Google Search platform relies on user-uploaded images for "reverse image search." Google, *Search for Images with Reverse Image Search* (2019), https://support.google.com/websearch/answer/1325808?hl=en&ref_topic=3180360.
[8] https://www.theverge.com/2018/7/25/17613442/google-drive-one-billion-users.

- a list of IP addresses used to access the user account (which can go as far back as the original account registration date);
- the user's secondary email address provided to Google to recover access to the Gmail account;
- the filename(s);
- the "categorization" of the image(s) based on an existing rubric; and
- a copy of the image file(s).

CyberTipline Report 5074778 at 3–12, ECF No 62-3, *United States v. Wilson*, No. 3:15-cr-2838, 2017 WL 2733879 (S.D. Cal. Jun. 26, 2017). The NCMEC system automatically adds data to the report by identifying the following information associated with the user's IP address(es): Country, Region, City, Metro Code, Postal Code, Area Code, Latitude/Longitude, and Internet Service Provider or Organization. *See, e.g.*, *id*. at 13–15. Then the NCMEC staff collect additional information, including "data gathered from searches on publicly-available, open-source websites" using the account and user identifying information provided in the CyberTipline Report. *See, e.g.*, *id.* at 16. The information NCMEC gathers can include social media profiles, websites, addresses, and other personal data. *See, e.g.*, *id.* at 6–11. All of this personal data would be collected and then sent to a

detective near the user before any person at Google or NCMEC has actually reviewed the files to confirm that they are contraband.[9]

There are at least three types of errors that could trigger the disclosure of a person's private data to a law enforcement agency where, in fact, no suspected contraband image was ever uploaded.

First, a Google employee could add the hash value of a non-contraband image to Google's suspected contraband repository (record entry error). A record entry error could arise when a Google employee mistakenly believes a non-contraband image contains contraband, or when the hash value of a contraband image is recorded incorrectly in the repository.

Second, a service provider might erroneously add an image's hash value to its suspected contraband repository based on a list of hash values that it received from some other entity (downstream error). The potential for downstream error was previously identified by the court in *United States v. Keith*, 980 F. Supp. 2d 33 (D. Mass. 2013), in a case where AOL's staff had not actually reviewed the original image that was the basis for the hash value.

Third, Google's algorithm could generate a false positive due to the specific image matching method used (match error). A false positive could, for example, be

[9] *See* McGoff Declaration, *supra*, ¶ 7 ("When Google's product abuse detection system encounters a hash that matches a hash of a known child sexual abuse image, in some cases Google automatically reports the user to NCMEC without re-reviewing the image.").

caused by similarities in the images even if one image contains suspected contraband and the other does not. The likelihood of a mismatch error depends entirely on the specific hashing method used and its false positive rate. For example, certain *file* hashing algorithms are designed "to confirm that when a copy of data is made, the original is unaltered and the copy is identical, bit-for-bit." Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 Harv. L. Rev. 38, 38 (2005). But there is no evidence on the record that Google's algorithm matches *files* bit-for-bit. In fact, it is highly unlikely that Google's algorithm assigns each file a unique hash value because slight changes to the file, e.g., by cropping or lightening the image, would alter the hash value and thereby evade detection by the algorithm. Other image matching techniques, including Microsoft PhotoDNA, which is used by NCMEC, identify "similar" images based on analysis of the image's content. Microsoft, *Photo DNA: Step-by-step*.[10] Google's algorithm most likely works in a similar way by manipulating the file and then assigning a value based on the image data. But Google has not explained what its algorithm does to an image file to set this value.

The Google declaration submitted in this case does not provide sufficient detail to evaluate the reliability and validity of their image matching technique or

[10] *Available at* https://web.archive.org/web/20130921055218/http://www.microsoft.com/global/en-us/news/publishingimages/ImageGallery/Images/Infographics/PhotoDNA/flowchart_photodna_Web.jpg (last accessed Sept. 21, 2013).

of their process for adding image values to the suspected contraband repository. In order to allow the ongoing scanning and reporting of images users upload to Google services, the Government should, at a minimum, be required to disclose the underlying evidentiary techniques and show that they are valid and reliable. A warrantless search of private files is unreasonable where the Government relies on a proprietary algorithm and fails to establish the reliability and accuracy of the technique.

II. Image matching techniques, like other investigative techniques, require research and testing to establish reliability.

A. On the record before this court, the Government cannot establish with "virtual certainty" that the files it searched were identical to the files that a Google employee previously viewed.

The lower court made a key mistake in the discussion of hashing technology when it relied upon an out-of-circuit case that cited a 2005 law review article discussing file hashing techniques. Mem. Order 2 n.2, ECF No. 57 (citing Salgado, *supra*, at 38–39).[11] What the court did not appreciate is that the file hashing techniques discussed in the Salgado article are fundamentally different from image matching techniques at issue in this case. The court's Fourth Amendment ruling was based on the premise that the image value created by Google's matching algorithm is equivalent to a "digital fingerprint," Mem. Order 2, and that an image

[11] Mr. Salgado is an attorney and was at that time a senior legal director at Yahoo!. He is now Google's Director of information security and law enforcement matters.

is "assigned a unique hash value." *Id.* at 10. But the Government has not disclosed or even described the Google image matching technique, and has not established that the system can match files with a virtual certainty. Without more information about the technique and evidence of accuracy and reliability, the court did not have the factual basis to reach that conclusion.

The *file hashing* techniques described in the Salgado article are used to *uniquely identify* or authenticate files and signatures; the *image matching* techniques deployed Google, Microsoft, and others are used to identify *similar features* in image files even if those files are actually different (e.g. if the color, orientation, or size, has been changed). *See* Microsoft, Digital Crimes Unit, *PhotoDNA* at 4 [hereinafter Microsoft PhotoDNA Slides].[12] While file hashing algorithms minimize false positives, files that have been modified or altered will necessarily produce different hash values. Bruce Schneier, *Applied Cryptography* 30 (1996) ("A single bit change in the pre-image changes, on the average, half of the bits in the hash value."). In contrast, image matching algorithms techniques are more likely to produce many false positives. These techniques attempt to match images even if the files have been altered, i.e., the files have different hash values. *See* Microsoft PhotoDNA Slides, *supra*, at 4. In other words, image matching

[12] *Available at* https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802f249e (last accessed Mar. 27, 2019).

techniques such as Microsoft's PhotoDNA do *not* assign unique hash values to files. Instead, these techniques analyze images to create a value that can be matched to many different files depending on the content of that file.

The technique of matching *files* relies on "one-way hash functions," which are commonly used in cryptographic systems. Schneier, *supra*, at 30. A hash function produces a message digest, which "distill[s] the information contained in a file (small or large) into a single large number, typically between 128 and 256 bits in length." Simson Garfinkel & Gene Spafford, *Web Security & Commerce* 202 (1997). Several message digest algorithms, including MD4 and MD5, were developed by Ronald Rivest,[13] while others (Secure Hash Algorithm, or SHA, and its revised version) were developed by the National Security Agency. *Id.* at 203–204. These functions are "powerful tools for detecting very small changes in very large files." *Id*. at 205. As cryptographer Bruce Schneier explains:

> Think of it as a way of fingerprinting files. If you want to verify that someone has a particular file (that you also have), but you don't want him to send it to you, then ask him for the hash value. If he sends you the correct hash value, then it is almost certain that he has that file.

Schneier, *supra*, at 31.

In contrast, *image matching* techniques are based on different functions and achieve different results. The value of an image is a "distinctive signature, which represents the visual content of the image in a compact way (usually just a few

[13] *See Ron Rivest, The MD5 Message-Digest Algorithm RFC 1321* (Apr. 1992).

bytes).” Sebastiano Battiato, Giovanni Maria Farinella, Enrico Messina, & Giovanni Puglisi, *A Robust Forensic Hash Component for Image Alignment*, 2011 Int’l Conf Image Analysis and Processing 473, 474 (2011). There are many different image matching techniques because each algorithm is designed to be “robust against allowed operations” while “at the same time” attempting to distinguish different and/or tampered images. *Id*. These “approximate matching” techniques are referred to as “perceptual hashing” because they aim to “detect objects that are perceptually similar from the perspective of a human.” Petter Christian Bjelland, Katrin Franke, & André Årnes, *Practical Use of Approximate Hash Based Matching in Digital Investigations*, 11 Digital Investigations S18, S20 (2014).

For example, PhotoDNA—an image matching function developed by Microsoft and Dartmouth College for use by NCMEC—can match images even if minor changes have been made that would change the file hash value, such as cropping, resizing, and adjusting the color. As Microsoft described at the time that it developed the PhotoDNA technique, “The PhotoDNA ‘robust hashing’ technique differs from other common hashing technologies because it does not require the image’s characteristics to be completely identical to reliably find matches, thereby enabling matches to be identified even when photos are resized or

similarly altered." Microsoft, *PhotoDNA: Fact Sheet* (2009).[14] One of the reasons that Microsoft itself cites for the use of its image matching technique is that it is capable of matching two images even if the files themselves are different. *See* Microsoft PhotoDNA Slides, *supra*, at 4.

Given the differences in the reliability of file hashing techniques and image matching techniques, courts should require the Government to provide specific evidence about an image matching method relied upon to justify a search. The Government cannot simply provide surface-level assertions of reliability and analogies to other forensic techniques. Without evidence about how the specific technique works, it is impossible to determine whether there was a "virtual certainty" that Google staff previously viewed the image files sent to NCMEC.

B. The National Academy of Sciences and other experts have raised significant concerns about the lack of reliable standards for investigative techniques.

EPIC's concerns about the courts' reliance on image matching techniques in this case arise in the context of a growing scientific and legal consensus about the need to assess the reliability of new investigative techniques. Forensic science has been widely criticized because of a lack of clear standards and credible research to support technical conclusions. *See* President's Council of Advisors on Science and

[14] *Available at* https://web.archive.org/web/20140323033617/http://www.microsoft.com/en-us/news/presskits/photodna/docs/photodnafs.doc.

Technology, *Forensic Science in Criminal Courts: Ensuring Scientific Validity of Feature-Comparison Methods* (2016) [hereinafter PCAST Report]; National Research Council of the National Academies, *Strengthening Forensic Science in the United States: A Path Forward* (2009) [hereinafter National Academy Report]. Even groundbreaking new methods that seem infallible should be subject to scrutiny. Erin E. Murphy, *Inside the Cell: The Dark Side of Forensic DNA*, at x–xi (2015). If the Government believes that Google's algorithm is reliable enough to meet the Fourth Amendment "virtual certainty" standard, then it should produce evidence of how the technique works and be able to assure this Court and others of the reliability and accuracy of the technique.

It is widely known throughout the criminal justice system that novel techniques, presented as scientific and infallible, are in fact flawed and imperfect. *See, e.g.*, Geoffrey C. Bunn, *The Truth Machine: The Social History of the Lie Detector* 5 (2012) ("[U]se of the machine has constantly transgressed the boundary that supposedly demarcates factual science from sheer fantasy.") The 2009 National Academy Report identified several significant problems in forensic science, including "the potential danger of giving undue weight to evidence and testimony derived from imperfect testing and analysis" and the subsequent "admission of erroneous or misleading evidence." National Academy Report at 4. The National Academy Report was commissioned by Congress to "identify the

needs of the forensic science community." *See* The Science, State, Justice, Commerce, and Related Agencies Appropriations Act of 2006. P.L. No. 109-108, 119 Stat. 2290 (2005).

The National Academy found that "The simple reality is that the interpretation of forensic evidence is not always based on scientific studies to determine its validity." National Academy Report, *supra*, at 8. The report discussed how several prominent forensic techniques that have "been called into question," including "fingerprint analysis." *Id*. at 43. Fingerprint identifications had been "viewed as exact means of associating a suspect with a crime scene print and were rarely questioned." *Id*. But the scientific foundation of this technique has now been called into question because it is not established that "one can determine with adequate reliability that the finger that left an imperfect impression at a crime scene is the same finger that left an impression (with different imperfections) in a file of fingerprints." *Id*. So the fact that the Government and courts have described these image matching values as a "digital fingerprint," Mem. Op. 3, shouldn't necessarily instill confidence. The Supreme Court has recognized the significance of the National Academy Report in identifying problems with the reliability of forensic methods. *See Melendez-Diaz v. Massachusetts*, 557 U.S. 305, 318 (2009).[15] This Court should also look to that report when considering what

[15] In full, the Court stated:

evidence is necessary to establish reliability of the image matching technique at issue in this case, and in other cases involving hash algorithms going forward.

The Supreme Court has recognized that, in the context of the Federal Rules of Evidence, a "trial judge must ensure that any and all scientific testimony or evidence admitted is not only relevant, but reliable." *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579, 589 (1993). The focus of a trial judge should be solely on "principles and methodology . . . ." *Id*. at 595. This presents a problem where "[f]orensic science facilities exhibit wide variability in capacity, oversight, staffing, certification, and accreditation across federal and state jurisdictions." National Academy Report at 14. The Report recommended that NIFS have an advisory board comprised of experts in "forensic science disciplines . . . information technology, measurements and standards, testing and evaluation, law,

---

> Nor is it evident that what respondent calls "neutral scientific testing" is as neutral or as reliable as respondent suggests. Forensic evidence is not uniquely immune from the risk of manipulation. According to a recent study conducted under the auspices of the National Academy of Sciences, "[t]he majority of [laboratories producing forensic evidence] are administered by law enforcement agencies, such as police departments, where the laboratory administrator reports to the head of the agency." National Research Council of the National Academies, Strengthening Forensic Science in the United States: A Path Forward 183 (2009) (hereinafter National Academy Report). And "[b]ecause forensic scientists often are driven in their work by a need to answer a particular question related to the issues of a particular case, they sometimes face pressure to sacrifice appropriate methodology for the sake of expediency." *Id.*, at 23–24. A forensic analyst responding to a request from a law enforcement official may feel pressure--or have an incentive--to alter the evidence in a manner favorable to the prosecution.

Melendez-Diaz, 557 U.S. at 318.

[and] national security . . . ."*Id*. The NIFS would be responsible for implementing standardized reporting, increasing research, developing best practices, and imposing quality control. *Id*. at 19–33.

A 2016 report from the President's Council of Advisors on Science and Technology ("PCAST"), which sought to clarify the scientific standards underlying the evidentiary rules established in *Daubert* and Rule 702, extended many of the conclusions from the National Academy Report. The PCAST report said that "answering the question of scientific validity in the forensic disciplines is important not just for the courts but also because it sets quality standards that ripple out throughout these disciplines—affecting practice and defining necessary research." PCAST Report at 43. The report described the requirement that evidence be based on "reliable principles and methods" to correspond to the scientific standard of "foundational validity." *Id*. Foundational validity requires that, "based on empirical studies," a method be "repeatable, reproducible, and accurate, at levels that have been measured and are appropriate to the intended application." *Id*. at 47. The report provided the following definitions of repeatable, reproducible, accurate, and reliable:

> By "repeatable," we mean that, with known probability, an examiner obtains the same result, when analyzing samples from the same sources.
> By "reproducible," we mean that, with known probability, different examiners obtain the same result, when analyzing the same samples.

> By "accurate," we mean that, with known probabilities, an examiner obtains correct results both (1) for samples from the same source (true positives) and (2) for samples from different sources (true negatives). By "reliability," we mean repeatability, reproducibility, and accuracy.

Id. The report stressed that "[t]he method need not be perfect, but it is clearly essential that its accuracy has been measured based on appropriate empirical testing and is high enough to be appropriate to the application." *Id*. at 48. PCAST made clear that mere assertions of certainty are insufficient: "Statements claiming or implying greater certainty than demonstrated by empirical evidence are scientifically invalid." *Id*. at 54.

A group of law professors, academic researchers, and practicing forensic scientists, led by Dean Jennifer Mnookin, have also sought to develop a common framework for modern forensics. *See* Jennifer L. Mnookin et al., *The Need for a Research Culture in the Forensic Sciences*, 58 UCLA L. Rev. 725 (2011). Dean Mnookin's study argues for an increased focus on empiricism, transparency, and the type of ongoing critical perspective inherent in a "research culture." *Id*. at 740-44.

In this case, the Government has failed to produce evidence describing the image matching technique or to establish the accuracy and reliability of that technique. This state of affairs is at odds with the views of the National Academies and leading experts to ensure the accuracy and reliability of forensic techniques.

C. The Government's prior use of flawed techniques to scan private messages underscores the need for proof of reliability here.

This is not the first time that the Government has purported to develop a technique that perfectly identifies evidence that falls outside the ambit of the Fourth Amendment. In the late 1990s, the FBI developed a software program called "Carnivore" to enable interception of Internet communications pursuant to a court order. *See Internet and Data Interception Capabilities Developed by FBI: Hearing Before the Subcomm. on the Constitution of the H. Comm. on the Judiciary*, 106th Cong. (2000) (statement of Donald M. Kerr, Assistant Director, Laboratory Division, Federal Bureau of Investigation). Carnivore was designed to act like a commercial packet "sniffer" product, which analyzes electronic communications packets as they travel through a network. *See id*. According to the agency, Carnivore could be configured to filter and then store "transmissions which comply with pen register court orders, trap & trace court orders, Title III interception orders, etc." *Id.* The Bureau claimed that, using this technique, only the communications subject to warrant authority would be obtained from the networks of private communications services.

The IIT Research Institute conducted an independent assessment of the FBI's program, and determined that the Carnivore software was capable of collecting "everything that passes by on the Ethernet segment to which it is connected." IIT Research Inst., *Independent Technical Review of the Carnivore*

System: Final Report 4-3 (2000) [hereinafter IITRI Final Report]. The Report also found that "Carnivore version 1.3.4 collects more than would be permitted by the strictest possible construction of the pen-trap statute," and the FBI "admitted that a previous version of Carnivore handled pipelined SMTP [packets] incorrectly." *Id*. However, the Report concluded that there were "significant procedural checks to minimize configuration errors." *Id*.

The proper configuration and use of the Carnivore software was thus a critical element of any legal use of the tool. *See Melendez-Diaz,* 557 U.S. at 318. As Professor Orin Kerr also noted, "legitimate concerns exist that the program may malfunction, and as with any tool, human error can cause the program to be configured incorrectly." Orin Kerr, *Internet Surveillance Law After the USA PATRIOT Act: The Big Brother That Isn't*, 97 Nw. U. L. Rev. 607, 654 (2003). In response to this concern, Congress added new reporting requirements under the pen register statute, codified at 18 U.S.C. § 3123(a)(3), that require documentation of:

> (i) any officer or officers who installed the device and any officer or officers who accessed the device to obtain information from the network;
> (ii) the date and time the device was installed, the date and time the device was uninstalled, and the date, time, and duration of each time the device is accessed to obtain information;
> (iii) the configuration of the device at the time of its installation and any subsequent modification thereof; and
> (iv) any information which has been collected by the device

18 U.S.C. § 3123(a)(3).

Without detailed information about the configuration or capabilities of a particular investigative technique, a court cannot determine whether it meets the standard of accuracy and reliability that the Government must establish under the Fourth Amendment.

* * *

Given the high bar established for the private search exception, this Court should require that the Government disclose information about the operation of Google's image matching technique, including the accuracy rate, and the number of false positives identified. The alternative is to allow the ubiquitous surveillance of Internet users for suspected contraband by a technique that is opaque, unaccountable, and lacking evidence of reliability or accuracy. Such a search must be deemed unreasonable.

CONCLUSION

The lower court did not understand the difference between a file hashing algorithm and an image matching technique. This Court should reverse because Google's routine scanning of the private files of Internet users for criminal referral, with a secret, unproven, and unaccountable technique, is unreasonable.

March 28, 2019

Respectfully submitted,

/s/ Marc Rotenberg
Marc Rotenberg
Alan Butler
Megan Iorio
Electronic Privacy Information Center
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140
Counsel for Amicus

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

Form 8. Certificate of Compliance for Briefs

Instructions for this form: http://www.ca9.uscourts.gov/forms/form08instructions.pdf

9th Cir. Case Number(s) 18-50440

I am the attorney or self-represented party.

This brief contains 5,593 **words**, excluding the items exempted by Fed. R. App. P. 32(f). The brief's type size and typeface comply with Fed. R. App. P. 32(a)(5) and (6).

I certify that this brief *(select only one)*:

- ○ complies with the word limit of Cir. R. 32-1.
- ○ is a **cross-appeal** brief and complies with the word limit of Cir. R. 28.1-1.
- ◉ is an **amicus** brief and complies with the word limit of Fed. R. App. P. 29(a)(5), Cir. R. 29-2(c)(2), or Cir. R. 29-2(c)(3).
- ○ is for a **death penalty** case and complies with the word limit of Cir. R. 32-4.
- ○ complies with the longer length limit permitted by Cir. R. 32-2(b) because *(select only one):*
  - ○ it is a joint brief submitted by separately represented parties;
  - ○ a party or parties are filing a single brief in response to multiple briefs; or
  - ○ a party or parties are filing a single brief in response to a longer joint brief.
- ○ complies with the length limit designated by court order dated _____.
- ○ is accompanied by a motion to file a longer brief pursuant to Cir. R. 32-2(a).

Signature s/ Alan Butler **Date** 03/28/2019

*(use "*s/[typed name]*" to sign electronically-filed documents)*

Feedback or questions about this form? Email us at forms@ca9.uscourts.gov

CERTIFICATE OF SERVICE

I hereby certify that on March 28, 2019, I electronically filed the foregoing Brief of *Amicus Curiae* Electronic Privacy Information Center in Support of Appellant with the Clerk of the United States Court of Appeals for the Ninth Circuit using the CM/ECF system. All parties to this case will be served via the CM/ECF system.

Dated: March 28, 2019

/s/ Alan Butler
Alan Butler