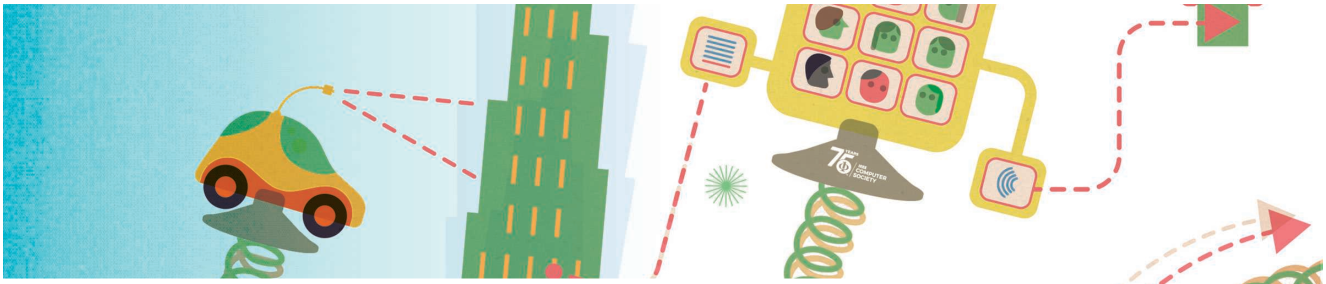
EIC'S MESSAGE

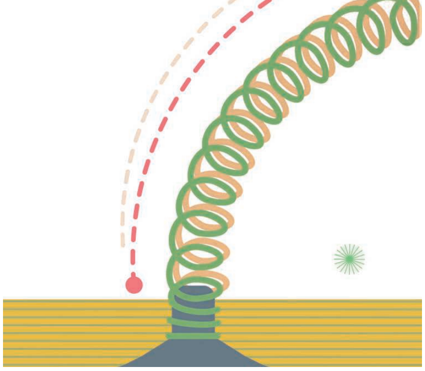
EDITOR IN CHIEF JEFFREY VOAS
IEEE Fellow; j.voas@ieee.org



Confronting Your Digital Accuser

Jeffrey Voas, IEEE Fellow

Keith Miller, University of Missouri at St. Louis



The blur between technology, the ability of the law and legislation to keep up, and the general distrust by the public has in anything from the mainstream or social media is brilliantly clear. We hope to begin a new conversation on this topic.

> *In all criminal prosecutions, the accused shall enjoy the right . . . to be confronted with the witnesses against him.* —U.S. Constitution, Sixth Amendment

If proprietary software accuses you of a crime, should you have the right to face your digital accuser in court? The "confrontation clause" in the U.S. Constitution has a history that traces back at least to the Roman Empire. However, a curious exception seems to occur if a "witness" against you is proprietary software. A recent example of this scenario is the Forensic Statistical Tool (FST).

FST was developed by New York City's Medical Examiner's Office, which started using it officially in 2011. It also sold the service to others, and, by 2017, FST had been used in 1,350 cases. The goal of FST is to analyze mixed samples of DNA collected at a crime scene and determine the probability that this mixture included a particular defendant's DNA. FST was designed to work with relatively small DNA samples and with mixtures of DNA from which it previously had been difficult to obtain results that were usable in court.

DNA has been used for decades in criminal trials, and its use is not generally controversial. However, newer analysis methods that use small amounts and mixed samples of DNA have become controversial. FST, in particular, has collected more than its share of detractors. After FST evidence was presented at trials, defense lawyers and their expert witnesses requested access to information about the FST program, including access to the source code and testing results. For years, such requests were routinely denied, largely because FST is proprietary software.

In 2016, the first expert review of FST was allowed by the courts, and the results were not pretty. The expert uncovered numerous problems; one particularly interesting "feature" was an undisclosed function that, according to the expert, was capable of dropping evidence that might be useful for the defense. Based on this expert opinion and in response to

Digital Object Identifier 10.1109/MC.2020.3038516
Date of current version: 9 April 2021

IN THIS ISSUE

For this April 2021 issue, we feature three articles. In "π-RT: A Runtime Framework to Enable Energy-Efficient, Real-Time Robotic Vision Applications on Heterogeneous Architectures," the authors discuss how stringent resource and energy constraints are major challenges for autonomous driving and robotics. They argue that developing domain-specific accelerators as proposed by others is costly as well as time consuming and, therefore, may not be suitable for immediate commercial deployment. They explain that the enormous computing power delivered by modern heterogeneous processors has not yet been fully exploited, and they demonstrate that even a simple runtime layer, π-RT, that dynamically dispatches the computationally intensive robotic vision operators can achieve significant performance and energy consumption improvements. With π-RT, they enable mobile robots to simultaneously perform autonomous navigation with 25 frames/s of localization, obstacle detection with 3 frames/s, route planning, large-map generation, and scene understanding, all within an 11-W computing power envelope.

In "Crowd–Machine Hybrid Urban Sensing and Computing," the authors look at how advances in the Internet of Things, artificial intelligence, and cloud/edge computing foster urban sensing and computing (USC). They claim that USC is becoming a promising solution to address significant challenges in modern cities. They investigate how to combine the power of human/crowd and machine intelligence to enable innovative applications of USC. Their article proposes a generic framework for crowd–machine hybrid USC, and they provide two applications in public health and environment monitoring as case studies.

In "Flipping the Script: A Sociotechnical Approach to Platforms and Unanticipated Uses," the author investigates social media platforms and how they can allow for unanticipated uses. The author argues that these platforms 1) display unique qualities that afford unanticipated uses and 2) challenge the application of human-centered evaluations and interpretations. The author claims that this observation, along with a rise in unanticipated uses, demonstrates that the design, function, and use of platforms are best treated as sociotechnical. Therefore, the author believes that the application of sociotechnical concepts should be used for evaluating unanticipated platform usages. The article offers real-world examples, including the dissemination of misinformation.

—Jeffrey Voas, Editor in Chief

Digital Object Identifier 10.1109/MC.2021.3057441
Date of current version: 9 April 2021

a motion by the publication *ProPublica*, the court allowed the copyrighted source code of FST to be publicly disclosed. The code is available at https://github.com/propublica/nyc-dna-software.

In 2018, a conviction involving FST evidence was overturned for the first time. Several other such cases are still being argued in the courts. However, many people who are incarcerated because of FST evidence may not be able to have their convictions overturned. Faced with DNA "evidence" based on FST, some defendants were advised by their lawyers to take a plea (for a lesser sentence) because such DNA evidence was thought to be difficult to overcome. Appealing a guilty plea is more difficult than appealing a guilty verdict that was contested.

In 2018, a conviction involving FST evidence was overturned for the first time. Several other such cases are still being argued in the courts.

Several aspects of FST interested us: its technical details, the problems with its testing, and the legal struggle to bring it out in the open. For more about these details, interested readers can see the article by Lacambra et al.[1]

At least two important issues will continue to be of concern long after the FST controversy ends:

1. When software produces outputs that are used as evidence in a criminal trial, is it ever fair to hide the details of that software from the defense? We know that the answer to that question was "yes" for years; we suspect that the answer should be "no."
2. A larger issue that is related to transparency for forensic DNA software is transparency for other software that can dramatically change people's lives. In the legal system, this includes DNA analyses but also software that advises the court

on things like sentencing and paroles. Outside the courts, software helps decide on loan eligibility, credit ratings, and medical diagnoses. Transparency seems important for these programs, too, especially if the software uses artificial intelligence techniques, the decisions of which can be difficult to trace or explain. For more information about this issue, please see the article by Matthews.[2]

DISCLAIMER

The authors are completely responsible for the content in this message. The opinions expressed are their own.

Look for more about these issues in future *Computer* articles. Because of their professional expertise, we expect that our readers, more than most people, are likely to understand how profoundly technical decisions about software transparency can affect people's lives and liberty. Please send your thoughts to us. ■

REFERENCES

1. S. J. Lacambra, J. Matthews, and K. Walsh. "Opening the black box: defendants' rights to confront forensic software." *The Champion*. pp. 28–30, 32–34, 38, 39, 66, May 2018. https://www.eff.org/document/opening-black-box-defendants-rights-confront-forensic-software
2. J. Matthews, "Patterns and anti-patterns, principles, and pitfalls: accountability and transparency in artificial intelligence," *AI Mag.*, vol. 41, no. 1, pp. 82–89, Winter 2019.

JEFFREY VOAS, Gathersburg, Maryland, USA, is the editor in chief of *Computer*. He is a Fellow of IEEE. Contact him at j.voas@ieee.org.

KEITH MILLER is the Orthwein Endowed Professor of Lifelong Learning in the Sciences at the University of Missouri at St. Louis, St. Louis, Missouri, 63121, USA. Contact him at keith.w.miller@umsl.edu.

Rejuvenating Binary Executables • Visual Privacy Protection • Communications Jamming
IEEE
SECURITY & PRIVACY
Building Dependability, Reliability, and Trust
SOFTWARE EVERYWHERE
January/February 2016 Vol. 14, No. 1
Policing Privacy • Dynamic Cloud Certification • Security for High-Risk Users
IEEE Symposium on Security and Privacy
March/April 2016 Vol. 14, No. 2
Smart TVs • Code Obfuscation • The Future of Trust
ECONOMICS OF CYBERSECURITY PART 2
May/June 2016 Vol. 14, No. 3
IEEE
IEEE computer society
CELEBRATING 70 YEARS
Reliability Society
S&P

Digital Object Identifier 10.1109/MC.2021.3066060