Editor: **Brittany Johnson**
George Mason University
johnsonb@gmj.edu

Editor: **Tim Menzies**
North Carolina State University
tim@menzies.us

Fighting for What's Right: An Interview With Marc Canellas

Brittany Johnson and Tim Menzies

From the Editors

Ethics is more than just a technical issue. Legal issues matter, too. To explore those legal issues, we talked to Dr. Marc Canellas—a proud public defender, engineer, and public policy advocate. As a public defender he defends people from the excesses of our legal and political systems, using his expertise in technology (he has a Ph.D. in aerospace and cognitive engineering) and policy (he is a former IEEE-USA Science and Technology Fellow for a Congressional House member and past chair of IEEE-USA's AI Policy Committee).

And for future issues we ask, "What do you want to see in this SE for Ethics column"? Do you have an important insight or industrial case study? Something that could prompt an important discussion? Or, alternatively, that extends or challenges significant ideas? If so, e-mail a one-paragraph synopsis to johnsonb@gmu.edu or timm@ieee.org (subject line: "SE for Ethics: Idea: [Your Idea]"). If that looks interesting, we'll ask you to submit a 1,000–3,000 word article (where each graph, table, or figure is worth 250 words) for review for *IEEE Software.—Tim Menzies*

You seem to have a unique professional perspective. Are you a lawyer? A test engineer? A policy advocate? If the three are connected, does that also mean you are now positioned to help those who might be hurt by poorly constructed software?

Marc Canellas: In many ways, I'm all three. As a public defender, my job is to advocate for the rights and humanity of people disfavored by most of society. But if you want to advocate for human and civil rights in our modern technological society, you have to advocate for software testing. As a researcher and policy advocate, I have long advocated for what I call *good design,*[1] for the baseline of ensuring that high-risk software works, that they are fit for their purpose and independently verified and validated (V&V)—writing about everything from AI,[2] autonomous weapons,[3] autonomous vehicles,[4] to complex, sociotechnical systems,[5] and electronic voting machines.[6,7]

Digital Object Identifier 10.1109/MS.2023.3340928
Date of current version: 22 February 2024

Software testing, independence, and V&V are fundamental principles of good design to engineers. But unfortunately, people are charged with crimes because of face recognition, DNA software, and many other technologies that are not tested according to those principles. We know they are not tested because when accused people object to evidence generated by these technologies or appeal their convictions due to poor software testing (or lack of independent testing), courts routinely deny these principles as necessary for ensuring the system's reliability which is a prerequisite for the evidence to be admissible. Courts have even gone so far as to say that somehow adherence to IEEE Standard 1012 for System, Software, and Hardware Verification and Validation can cause errors.[8] In the criminal legal system, it is an outlier opinion to believe that *before* the government uses software to justify taking away citizens' life and liberty, they should *first* ensure that it is independently verified and validated to be fit for its purpose.

Testing is absolutely essential because no technology is "neutral" (he says using air quotes). For example, I was previously a public defender in Arlington County, VA. Arlington County is over 70% White and one of the wealthiest counties in the country. While there, our office represented over 70% of the people charged with crimes, and yet every single one of our clients were in poverty (total assets and annual income less than US$18,000), and almost every one of those was Black or Hispanic. In a very wealthy, majority-White county, a majority of those being arrested were poor people of color.

So when we think about how these technologies are being used and upon whom they are being used, "neutral" doesn't get us very far. How does it work? How is it being used? Upon whom? What are the outcomes? What is the likelihood and consequences of failure? These are the essential questions for understanding if a technology is fit for its purpose—questions that independent testing, verification, and validation under IEEE Standard 1012 will answer. When a technology is used almost exclusively to surveil, target, and incarcerate marginalized groups such as people in poverty or people of color, the public and people being accused must be given answers to those essential questions.

ABOUT DR. MARC CANELLAS

Dr. Marc Canellas, public defender, engineer, and policy advocate, strives to make society more just and equitable one client, one technology, and one system at a time. Dr. Canellas is a public defender in the Forensics Division of the Maryland Office of the Public Defender. For more on Dr. Canellas, see https://www.linkedin.com/in/marccanellas.

Dr. Marc Canellas.

> We now have *thousands* of people who are in prisons right now, because of a DNA software that we know did not work.

When talking to you, or reading your papers, you speak about the criminal legal system and the impact technology has on real lives—especially the impact of poorly designed or untested software on real lives. Tell us about your work on DNA testing software.

Canellas: DNA evidence is devastating in court. I have been in trials where trace DNA evidence allegedly the result of a single touch of a victim's jeans was enough to place a person at a scene and guarantee a jury's conviction for robbery despite there being no identification by the victim, witnesses, videos, or other physical evidence. This analysis is a product of probabilistic genotyping (or DNA) software (like the Forensic Statistical Tool (FST), STRmix, and TrueAllele) which claim to identify people based on traces of DNA. These technologies are the most potent and egregious violators of engineering principles.

For example, FST was developed in 2011. There are no agencies or regulators ensuring software like this actually works, so that was left to criminal defense attorneys, like me. For years, we advocated for good design and independent testing of the software. This is where a criminal defense attorney and a software engineer are one and the same. Only in 2016 did an accused person and his independent testers get access to the software. Turns out, FST was not working the way the prosecution and the developers told the court the software worked.[8] It had indefensible statistical methods. Its assumptions did not match real-world operational environments. It was not even built by software engineers, but rather by forensics scientists who have little to no experience in statistics, let alone making production-quality software. Ultimately, after six years and thousands of cases, FST was found to be illegitimate, indefensible, and abandoned.

> The courts should, in accordance with IEEE Standard 1012, require independent verification and validation and public disclosure.

But even when a specific forensic software like FST is abandoned, the structure of our criminal legal system can make it a hollow victory. When people appealed their prior convictions based on FST evidence, judges rejected the appeals, saying "Yes, now we know the trial court was wrong to allow this software. Yes, now we know we should have required independent testing. But at the time, the trial court did not think that testing was necessary. Because the trial court didn't intentionally do anything wrong, they didn't abuse their discretion, and your conviction stands." So, we now have *thousands* of people—human beings with families, dreams—who are in prisons right now, because of a DNA software that we know did not work. People's lives are irreparably harmed, and victims are not able to get justice, all because developers deployed software that did not work, and prosecutors and the courts did not require the necessary testing before it was deployed.

Moreover, FST was replaced by new software like STRmix and TrueAllele which has not undergone any more independent testing than FST. So accused people and their attorneys have to start all over again arguing for independent testing of these technologies. This software, and others like face recognition software or ShotSpotter, are deployed in thousands of prosecutions without independent testing. Each day, criminal defense attorneys across the country stand up in court simply trying to ensure that before software is used to take away lives and liberty, we at least make sure they work.

So, what should we do differently?

Canellas: Legally and politically speaking, as IEEE-USA, IEEE Standards Association, and the IEEE Computer Society has made absolutely clear that policymakers and the courts should, in accordance with IEEE Standard 1012, require independent verification and validation and public disclosure of the results as a prerequisite for any software evidence used in a high-risk situation that can cause loss of life, liberty, or extensive financial or social loss.[9,10,11] This includes everything from criminal cases and family abuse and neglect proceedings, to school choice and tax enforcement.

But as engineers, the best thing you can do is be a good engineer and show up when and where it counts. Theodore von Kármán said that "we, engineers, create the world that has never been." We live in a world where nearly every decision affecting our lives is made through software. And yet, the U.S. has never required independent testing in the ways necessary to sufficiently protect our rights and liberties. All of us live at the mercy of untested, unreliable software that can falsely place us at the scene of a crime and cause us to lose our rights and liberties at any moment, without any protections or redress for error.

But you do not have to specialize in engineering ethics, and you certainly do not need to go to law school to make a difference. What you should do is stand up for engineering principles. You should support policies like those above. You should try to gain access to forensic software and test them yourself. You should take the call from the attorney asking for help and advice. We engineers have an obligation to make sure our society understands and respects the importance and value of independent testing.

To say this all another way, through your commitment to independent testing, you can create a more fair, just, and equitable world. You can create a world that has never been.

ABOUT THE AUTHORS

BRITTANY JOHNSON is an assistant professor in computer science at George Mason University, Fairfax, VA 22030 USA. Contact her at johnsonb@gmu.edu.

TIM MENZIES is a full professor at North Carolina State University, Raleigh, NC 27606 USA. Contact him at timm@ieee.org.

References

1. M. Canellas, "Oversight - follow up on local law 49 of 2018 in relation to automated decision systems used by agencies," New York City Council Committee on Technology New York, NY, USA, 2020. [Online]. Available: https://ieeeusa.org/assets/public-policy/committees/aipc/Canellas_Jan2020_NYCCTestimony.pdf
2. K. Katsikopoulos and M. Canellas, "Decoding human behavior with big data? Critical, constructive input from the decision sciences," *Ai Mag.*, vol. 43, no. 1, pp. 126–138, 2022, doi: 10.1002/aaai.12034.
3. M. Canellas and R. Haga, "Lost in translation: Building a common language for regulating autonomous weapons," *IEEE Technol. Soc. Mag.*, vol. 35, no. 3, pp. 50–58, Sep. 2016, doi: 10.1109/MTS.2016.2593218.
4. M. Canellas and R. Haga, "Unsafe at any level," *Commun. ACM*, vol. 63, no. 3, pp. 31–34, 2020, doi: 10.1145/3342102.
5. M. Canellas, M. Miller, Y. Razin, R. Haga, D. Minotra, and R. Bhattacharyya, "Framing human-automation regulation: A new modus operandi from cognitive engineering," WeRobot, 2017. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3567175
6. M. Canellas, "Voting machines must become more usable: Lots of voting machines are really confusing, and on election day, it showed," *Slate*, Nov. 20, 2018. Accessed: Dec. 20, 2023. [Online]. Available: https://slate.com/technology/2018/11/voting-machines-usability-election-day-confusing.html
7. M. Canellas. "Was your voting machine hacked? Without more user-friendly devices, we may not know." Just Security. Accessed: Dec. 20, 2023. [Online]. Available: https://www.justsecurity.org/61503/voting-machine-hacked-user-friendly-devices/
8. M. Canellas, "Defending IEEE software standards in federal criminal court," *Computer*, vol. 54, no. 6, pp. 14–23, Jun. 2021, doi: 10.1109/MC.2020.3038630.
9. IEEE-USA, IEEE Standards Association (IEEE SA), and the IEEE Computer Society, "RFC response: Digital investigation techniques: A NIST scientific foundation review (NISTIR 8354-DRAFT)," NIST, Gaithersburg, MD, USA, Rep. 8354, Nov. 2022.
10. IEEE-USA and IEEE Standards Association (IEEE SA), "RFC response: NIST internal report 8351-DRAFT DNA mixture interpretation: A NIST scientific foundation review," NIST, Gaithersburg, MD, USA, Rep. 8351, Nov. 2021.
11. J. Matthews, B. Hedin, and M. Canellas, "Trustworthy evidence for trustworthy technology: An overview of evidence for assessing the trustworthiness of autonomous and intelligent systems," IEEE-USA, Piscataway, NJ, USA, Sep. 29, 2022. [Online]. Available: https://ieeeusa.org/assets/public-policy/committees/aipc/IEEE_Trustworthy-Evidence-for-Trustworthy-Technology_Sept22.pdf