Testimony of

Rebecca Wexler

July 19, 2022

Statement of Rebecca Wexler
Co-Director, Berkeley Center for Law and Technology
Assistant Professor of Law, University of California, Berkeley, School of Law
Before the House Judiciary Committee
July 19, 2022

Mr. Chairman and members of the Committee. My name is Rebecca Wexler and I am a Faculty Co-Director of the Berkeley Center for Law and Technology and an Assistant Professor of Law at the University of California, Berkeley, School of Law. I am honored to have been invited to testify today about how law enforcement collection of data through private intermediaries can conceal evidence of innocence by circumventing criminal defense discovery rights.

To help fix this problem, Congress should consider ways to protect defense counsel's access to exculpatory evidence. For instance, eliminate the trade secret evidentiary privilege for private entities that sell data and investigative or forensic software to law enforcement.[1] Clarify that the Stored Communications Act and other federal privacy statutes do not block criminal defense subpoenas to technology companies.[2] Strengthen defendants' general third-party subpoena powers.[3] And require law enforcement to obtain evidence of innocence on behalf of the accused if defense counsel is unable to obtain it directly.[4]

Zooming out, discussions of law enforcement collecting data from private entities often address whether law enforcement may circumvent the Fourth Amendment to get more or easier access

[1] For a model bill performing this urgent reform, *see* The Justice in Forensic Algorithms Act of 2021, H.R. 2438, 117th Cong. § 2(b) (2021). For a detailed discussion of the trade secret evidentiary privilege and why it should not apply in criminal cases, *see* Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343 (2018).

[2] For arguments that the Stored Communications Act has been misinterpreted by the courts to erroneously create an evidentiary privilege blocking criminal defense subpoenas, *see* Rebecca Wexler, *Privacy as Privilege: The Stored Communications Act and Internet Evidence*, 134 HARV. L. REV. 2721 (2021). For a more general discussion of privacy statutes that asymmetrically block criminal defense access to data while permitting such access for law enforcement, *see* Rebecca Wexler, *Privacy Asymmetries: Access to Data in Criminal Defense Investigations*, 68 U.C.L.A. L. REV. 212 (2021).

[3] *See* FED. R. CRIM. P. 17.

[4] Nothing in current constitutional or federal law clearly requires law enforcement to seek out evidence of innocence beyond that known to the prosecution team, even if defense counsel is otherwise unable to obtaining the evidence. *See, e.g.*, Rebecca Wexler, *The CLOUD Act and the Accused*, Knight First Amendment Institute at Columbia University (July 19, 2022), https://knightcolumbia.org/content/the-cloud-act-and-the-accused-2.

to evidence of guilt than they would otherwise be able to get by seizing data directly.[5] Those conversations are important. At the same time, an underappreciated aspect of privatized evidence collection is that it also allows law enforcement to obtain less evidence of innocence. And when law enforcement does not possess exculpatory evidence, it is much harder for the defense to access it. This is what I am going to talk about today.

Let me provide some examples of this problem.

When law enforcement officers purchase data from intermediaries, or use private biometric databases, or license surveillance software from private companies, the officers can stay ignorant of flaws in the data. They do not have to learn whether the data were acquired in violation of a privacy statute. Or through breach of contract. Or through unlawful hacking. They do not have to learn about errors in quality control that could have corrupted the data. Or rendered it unreliable. Or subject to tampering. They do not have to learn about bugs, or improper validation studies, or racial, gender, and other biases in the software used to acquire the data. Indeed, private companies sometimes claim this type of information is a trade secret, and refuse to disclose it even to their own law enforcement customers or in response to a subpoena.

Yet all that information could be exculpatory evidence relevant to prove innocence and stop wrongful convictions. If law enforcement seizes data directly, they are much more likely to know this information. If they acquire data from private entities, they are much more likely not to. And when law enforcement is ignorant of flaws in their data, or in the data collection methods, it is harder for defendants to access that exculpatory evidence.

Here is why.

If law enforcement is ignorant of exculpatory evidence, defendants' constitutional *Brady* due process rights, which would otherwise require the prosecution to disclose evidence of innocence, will not apply.[6] Defendants' statutory discovery rights to obtain exculpatory evidence from the prosecution will not apply.[7] And if defendants exercise their Sixth Amendment rights to call law enforcement officers to the witness stand, cross-examination will be futile.

Meanwhile, current evidence rules permit prosecution witnesses to introduce data into evidence even if they are ignorant about flaws in the data or the method of collecting it. Most

---

[5] *See, e.g.*, Orin S. Kerr, *Buying Data and the Fourth Amendment*, Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 2109 (November 17, 2021), https://www .lawfareblog.com/buying-data-and-fourth-amendment.

[6] The Supreme Court has held that prosecutors have an affirmative duty under the *Brady* doctrine "to learn of any favorable evidence known to the others acting on the government's behalf in the case, including the police." *Kyles v. Whitley*, 514 U.S. 419, 437 (1995). But this duty does not extend to favorable evidence known by private entities not acting on the government's behalf.

[7] *See* FED. R. CRIM. P. 16.

courts say software does not trigger the hearsay bar or the Confrontation Clause.[8] You have to make a minimal showing that the data are authentic,[9] and for expert evidence you have to make a minimal showing of reliability,[10] but you can easily satisfy those requirements without learning about flaws in your own evidence.

Nor is it easy for defendants to get information about such flaws directly from a private company. In a catch-22, defendants cannot subpoena companies directly for exculpatory evidence unless they already know the evidence exists and can identify it with specificity—a task that is virtually impossible for evidence one has not yet seen.[11] And trying to get criminal defense subpoenas enforced across state lines can be prohibitively costly and time consuming.

Further, private vendors of surveillance technologies sometimes say their products are for law enforcement only, and refuse to give or sell copies to criminal defense experts for scrutiny and testing.[12] Indeed, some companies even refuse research licenses to independent scientists to scrutinize and test their products, all the while claiming in court that those products are subject to peer review.[13]

In sum, it is much harder for criminal defense counsel to access exculpatory evidence about flaws in data collected through private intermediaries than in data collected directly by law enforcement searches and seizures. The result not only risks wrongful convictions, it also exacerbates existing inequities in the U.S. criminal legal system. As the Innocence Project has reported, "the majority of wrongfully convicted people are those who are already among the most vulnerable in our society—people of color and people experiencing poverty."[14] The harms from concealing evidence of innocence through privatized collection will disproportionately fall on these underserved and historically marginalized communities.

Thank you for the opportunity to testify today. I look forward to your questions.

---

[8] *See, e.g.*, United States v. Lizarraga-Tirado, 789 F.3d 1107, 1109-10 (2015). *But see* Andrea Roth, *Machine Testimony*, 126 YALE L.J. 1972 (2017) (critiquing the current doctrine).

[9] FED. R. EVID. 901.

[10] FED. R. EVID. 702.

[11] *See* United States v. Nixon, 418 U.S. 683, 700 (1974) (imposing onerous requirements for obtaining a pre-trial Rule 17 subpoena).

[12] *See, e.g.*, https://www.grayshift.com/ ("GrayKey is restricted to local, state, and federal law enforcement, public safety, and defense agencies in select countries."); Letter from Justin Fisher, Grayshift Co-Founder, to Federal Communications Commission, May 13, 2020, https://fcc.report/FCC-ID/2AV7EGK01/4806655.pdf ("GrayKey is a specialized device sold only to verified law enforcement or government agencies and is not available for sale to the general public.").

[13] *See* GAO Report, https://www.gao.gov/assets/gao-21-435sp.pdf.

[14] Daniele Selby, *How Racial Bias Contributes to Wrongful Conviction*, The Innocence Project (June 17, 2021), https://innocenceproject.org/how-racial-bias-contributes-to-wrongful-conviction/. Over two-thirds of Innocence Project exonerees are people of color and 58% are Black. *Id.*