COMMENTS OF THE AMERICAN CIVIL LIBERTIES UNION, THE ELECTRONIC FRONTIER FOUNDATION, AND THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

National Highway Traffic Safety Administration

On

Advanced Impaired Driving Prevention Technology

89 Fed. Reg. 830 / Docket No. NHTSA-2022-0079

March 5, 2024

The American Civil Liberties Union (ACLU), the Electronic Frontier Foundation (EFF), and the Electronic Privacy Information Center (EPIC) submit these comments in response to the National Highway Traffic Safety Administration's advance notice of proposed rulemaking on a new Federal Motor Vehicle Safety Standard for "advanced drunk and impaired driving prevention technology."[1]

We appreciate the NHTSA's recognition of the importance of protecting privacy in the creation of an advanced drunk driving prevention (hereafter, DDP) technology rule, and its solicitation of generalized input on relevant privacy considerations prior to the issuance of future regulatory proposals. We believe that to ensure public acceptance, among other reasons, it is important to ensure that a DDP system cannot have consequences for people outside of

[1] 88 Fed. Reg. 830, https://www.federalregister.gov/documents/2024/01/05/2023-27665/advanced-impaired-driving-prevention-technology .

protectively addressing their impairment. In the sensitive area of personal alcohol consumption, that means airtight privacy protections.

For more than 100 years, the ACLU has been our nation's guardian of liberty, working in courts, legislatures, and communities to defend and preserve the individual rights and liberties that the Constitution and the laws of the United States guarantee everyone in this country. The ACLU takes up the toughest civil liberties cases and issues to defend all people from government abuse and overreach. The ACLU is a nationwide organization that fights tirelessly in all 50 states, Puerto Rico, and Washington, D.C., for the principle that every individual's rights must be protected equally under the law, regardless of race, religion, gender, sexual orientation, disability, or national origin.

EFF works to ensure that technology supports freedom, justice, and innovation for all the people of the world. EFF was founded in 1990 and has more than 30,000 members. It is a nonprofit organization that advocates before courts and legislatures to protect the privacy of technology users and consumers from corporations that collect and monetize their personal information.

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 secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation.[2] EPIC routinely advocates for strong privacy protections in transportation technologies, especially where those technologies collect sensitive data like location and biometric information.[3]

[2] EPIC, "About EPIC," https://epic.org/epic/about.html.
[3] *See e.g.*, EPIC, "Testimony to Maryland House Environment and Transportation Committee on Privacy Protections for Automated Ticketing Systems" (Feb. 29, 2024), https://epic.org/documents/epic-testimony-to-maryland-house-environment-and-transportation-committee-on-privacy-protections-for-automated-ticketing-systems/; EPIC, "Coalition Letter to DEA on unauthorized National License Plate Reader Program" (Mar. 8, 2023), https://epic.org/wp-content/uploads/2023/03/Coalition-Letter-DEA-ALPR-Program-March2023.pdf; EPIC,

Background

In the 2021 Infrastructure Investment and Jobs Act, Congress directed NHTSA to require that passenger motor vehicles manufactured after a certain date contain "advanced drunk and impaired driving prevention technology."[4] Although such a technology did not exist, and still has not been fully developed, Congress defined it as a system that can either "passively monitor the performance of a driver" to detect if they are impaired, or "passively and accurately detect" whether the driver's blood alcohol level is above the legal limit. If impairment or an illegal blood alcohol limit is detected, the system is required to "prevent or limit motor vehicle operation."

Some states already require in-car breathalyzers for people with DUI convictions.[5] Known as "ignition interlock devices," they require drivers to blow an alcohol-free breath into a tube before their car will start. But Congress directed that the technology be "passive," which appears to mean that no special action on the part of drivers should be necessary for the system to work.

NHTSA proposes several technological approaches to "passive" impaired or distracted driving detection in the ANPRM. One is a touch sensor that uses infrared spectroscopy to measure the concentration of alcohol in the capillary blood in the skin on a driver's palm using an optical touch pad integrated into a vehicle's ignition switch or steering wheel.[6] A second approach is a breath sensor similar to those that are already used for ignition interlock devices

---

"Comments to Transportation Department on Enhancing Safety for Vulnerable Road Users" (Nov. 15, 2022), https://epic.org/documents/epic-comments-enhancing-safety-for-vulnerable-road-users/; EPIC, "Location Tracking," https://epic.org/issues/data-protection/location-tracking/.

[4] Infrastructure Investment and Jobs Act, Pub. L. 117–58, 135 Stat. 429 § 24220 (2021).

[5] National Conference of State Legislatures, "State Ignition Interlock Laws" (last updated Sept. 24, 2021), https://www.ncsl.org/transportation/state-ignition-interlock-laws (44 total states have some form of interlock requirement for people with DUI convictions).

[6] The DADSS project palm sensor, 89 Fed. Reg. 844.

and law enforcement roadside testing devices.[7] Unlike those devices, the device would seek to passively measure the driver's natural exhalations — and distinguish those from the breath of possibly intoxicated passengers. These two technologies, NHTSA concludes, are the furthest along in development.

Another research thrust focuses on the use of vehicle-based algorithms to try to identify impairment. These systems would be based on some combination of cameras or other sensors inside a vehicle to monitor a driver, and monitoring of the driver's actual driving performance such as lane position consistency.[8] Driver monitoring technologies might include monitoring of facial features such as eye openness and closure, eye tracking, and body position. These approaches are still being researched.

I. The importance of protecting privacy in a drunk driving protection system

As residents of the United States, we recognize the terrible tragedy that drunk driving inflicts on too many people every year. As privacy advocates, we point out that while a DDP system could be a privacy nightmare, with some care the benefits of such technology can be obtained without invading Americans' privacy, and that privacy invasions are not necessary to exploit the potential benefits technology has to offer here.

Any technology that fulfills the Congressional mandate will likely collect sensitive data about drivers' bodies. That may include physiological data unrelated to intoxication level, as well as the fact that a person was intoxicated and tried to drive. No potentially invasive

[7] The DADSS project breath sensor, *Id*.
[8] *See e.g.* the DrIIVE project, 89 Fed. Reg. 845.

technology should be implemented that doesn't strongly protect sensitive data.[9] A poorly designed system could become a privacy nightmare. The purpose of this system is not forensic — it is not to help catch and prosecute drunk drivers or attempted drunk drivers. The purpose is to deter or prevent drunk people from driving at all. Given that the bulk of the safety benefits of DDP technology should be obtainable without privacy invasions, it would be unacceptable to introduce privacy violations to achieve these results.

There are several reasons why it's important to maintain privacy for everyone involved.

First, it is important to protect privacy for its own sake. Privacy is a vital value in a free and democratic society, where true freedom is impossible if people can't live their lives free from undue scrutiny by the state, powerful corporations, and the community at large.

Second, it's important to protect people from the concrete harms that privacy invasions can bring — for example, the repurposing of data collected by DDP tech for the purposes of corporate profiling, or for law enforcement purposes including potentially those unrelated to illegal driving under the influence of alcohol. It's important to protect Americans from the use of technology to unduly expand the reach of law enforcement surveillance and power into everyday life. That includes members of historically disadvantaged communities, such as Black people, against whom the criminal justice system remains biased at every level.[10]

---

[9] For example, recorded eye movements can be used for low-accuracy diagnosis of depression. Sharifa Alghowinem et al, "Eye movement analysis for depression detection," 2013 IEEE International Conference on Image Processing 4220 (2013), https://ieeexplore.ieee.org/abstract/document/6738869; Diabetic neuropathy may be diagnosed from recorded eye movements: Luis David Avendaño-Valencia et al, "Video-based eye tracking performance for computer-assisted diagnostic support of diabetic neuropathy," 114 *Artificial Intelligence in Medicine* (April 2021), https://www.sciencedirect.com/science/article/abs/pii/S0933365721000439. Neurodegenerative disease may be diagnosed at least in part from eye movements: Yuxing Mao et al, "Disease Classification Based on Eye Movement Features With Decision Tree and Random Forest," 14 *Frontiers in Neuroscience* 798 (2020), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7423879/.

[10] Racial disparities and bias are common across traffic enforcement including drunk driving enforcement, traffic stops, vehicle searches resulting from traffic stops, arrests, and prosecutions. Danielle M. Rousseau & Gerald P. Pezzullo Jr., "Race and Context in the Criminal Labeling of Drunk Driving Offenders: A Multilevel Examination of Extralegal Variables on Discretionary Plea Decisions," 25 *Criminal Justice Policy Review* 683 (2014),

Third, and perhaps of most direct concern to the NHTSA's mission, it's important to protect privacy if the agency wishes to maximize the public acceptability of a DDP regime. Americans have a very personal relationship with their cars. People's activities in their vehicles can have grave consequences for other people, which is why vehicles licensed for operation on public roadways are justifiably highly regulated. But they are nonetheless an intimate part of people's lives and are regarded as quasi-private spaces. Americans are not accustomed to having the arm of the state reach into their vehicles to monitor them, and whether justified or not as a public policy matter, many may reject such a concept. Indeed if a DDP system is self-contained, and cannot leak data outside the vehicle, then it will not actually consist of the "arm of the state," but merely as the operation of the vehicle.

End-user trust and the legitimacy of DDP technology may mean the difference between broad acceptance of that technology, and whatever consequent increases in road safety it may bring about, and widespread disabling, tampering, hacking, circumvention, and interference with these systems, which are likely to greatly complicate the implementation of this technology and undercut its goals.[11]

If privacy advocates cannot honestly report to the public that a DDP system has been designed with airtight privacy protections built in and cannot have consequences for people besides blocking their ability to drive their vehicle when they are impaired, that is likely to

---

https://journals.sagepub.com/doi/10.1177/0887403413493089; ACLU of Illinois, "Black and Latino Motorists in Illinois Continue to Experience Higher Rates of Traffic Stops According to New Data" (Jul. 13, 2023), https://www.aclu-il.org/en/press-releases/black-and-latino-motorists-illinois-continue-experience-higher-rate-traffic-stops; Emma Pierson et al; "A large-scale analysis of racial disparities in police stops across the United States," 4 *Nature Hum. Behav.* 736 (May 4, 2020), https://www.nature.com/articles/s41562-020-0858-1.

[11] For an example of a current countermeasure to a vehicle safety feature *see,* Faiz Siddiqui, "Tesla owners are using steering-wheel weights to drive hands-free," *Washington Post* (Jul. 7, 2023), https://www.washingtonpost.com/technology/2023/07/07/tesla-fsd-autopilot-wheel-weights/.

greatly add to popular resistance against this technology and be counter-productive as a safety measure.

II. Three core principles for protecting privacy in a drunk driving protection system

There are many potential privacy ramifications of a DDP system, depending on the technology adopted, but at this stage in the NHTSA's deliberations, we suggest three core principles for ensuring that privacy is protected.

1. Data storage must be minimized

Given that a DDP technology is likely to store physiological data about drivers, including potentially data unrelated to a driver's level of impairment, such as baseline measurements, it is important that the storage of any data be proportional to the safety benefits of the system and kept to the minimum level necessary for achieving those benefits.

If data is stored that is not required for the system to achieve its benefits, that immediately raises the question of why it is being retained, and the suspicion that it could be repurposed for other goals, including to benefit other parties with interests that are antagonistic to the driver's. Creating a honeypot of potentially sensitive yet valuable data increases the incentive for hackers to access that data and the consequences of such hacking. It also increases the incentive for unethical automakers, original equipment manufacturers (OEMs) or other parties to access the data. It is worth a reminder that Volkswagen was caught (and subsequently admitted to) including computer code in its vehicles that illegally tricked regulators' emissions testing

equipment in order to hide its evasion of environmental laws.[12] Given a strong incentive to obtain valuable personal data, suspicions of data access are likely to persist if such data is retained — even if every company involved actually behaves scrupulously — undermining public confidence in the operation of the DDP technology in people's cars.

Minimizing data collection is important, but so is minimizing data retention periods. A system that holds onto data for a few minutes is much harder to abuse than one that keeps sensitive personal information for months or years. These concerns are especially acute given the Biden Administration's recent investigation into the national security risks of data collection from connected cars.[13]

The data retained by a system should not only be minimized in scope and duration, but should also be proportional to the system's safety benefits. For example, a vast increase in the scope, duration, and sensitivity of data storage would not be justified by a small marginal increase in safety.

2. The data must not leave the car

We see no reason why any data collected for a DDP system needs to leave the vehicle, and accepting a system in which that is able to happen will greatly magnify the number, weight, and complexity of the privacy issues raised by DDP technology. NHTSA should require that data remain localized within the DDP system, and that such localization be built into the architecture

[12] Wikipedia, Volkswagen emissions scandal, https://en.wikipedia.org/wiki/Volkswagen_emissions_scandal; Jack Ewing, "Engineering a Deception: What Led to Volkswagen's Diesel Scandal," *New York Times* (Mar. 16, 2017), https://www.nytimes.com/interactive/2017/business/volkswagen-diesel-emissions-timeline.html.

[13] White House, "FACT SHEET: Biden-Harris Administration Takes Action to Address Risks of Autos from China and Other Countries of Concern" (Feb. 29, 2024), https://www.whitehouse.gov/briefing-room/statements-releases/2024/02/29/fact-sheet-biden-harris-administration-takes-action-to-address-risks-of-autos-from-china-and-other-countries-of-concern/.

and technology of such systems so that the distribution of data outside the vehicle isn't merely prohibited by policy, but is technologically impossible.

Car data storage systems should be modeled on another sophisticated technical system that contains and works with sensitive data about its users: smartphones with biometric unlock capabilities. These devices typically store information about their users' fingerprints or faces, but the most sophisticated and trustworthy devices do this in such a way that the system cannot release user biometric data to anyone at all.[14] Why mandate deployment of any DDP system that fails to live up to this widespread baseline?

The automobile industry is currently engaging in an illegitimate and unethical level of spying on vehicle owners, drivers, passengers, and even people who happen to be nearby.[15] Increasingly sophisticated computer systems monitor and control today's cars and trucks — and record data about every aspect of their operation, including sensitive data such as location, driving behavior, images, video, and the use of in-car data services. That data is routinely transmitted from vehicles to their manufacturers and other companies, who share it with various brokers and other middlemen to be analyzed for consumer profiling and marketing purposes. Very few drivers are currently aware of this, let alone have given permission for it in any meaningful way; nor is it clear that most vehicle owners can easily stop this flow of data. And the car companies refuse to answer questions about these practices.[16] At its worst, abusive data collection enables stalking and other direct harms to individual safety.[17]

---

[14] Apple, "About Touch ID advanced security technology" (Nov. 15, 2023), https://support.apple.com/en-us/105095; Google, Support, Understand fingerprint security (last accessed Mar. 4, 2024), https://support.google.com/pixelphone/answer/6300638?hl=en.

[15] "Tesla workers shared 'intimate' car camera images, ex-employees allege: 'Massive invasion of privacy,'" *The Guardian* (Apr. 7, 2023), https://www.theguardian.com/technology/2023/apr/07/tesla-intimate-car-camera-images-shared.

[16] Jen Caltrider, Misha Rykov, & Zoe MacDonald, "It's Official: Cars Are the Worst Product Category We Have Ever Reviewed for Privacy," Mozilla Foundation (Sept. 6, 2023),

Therefore, not only is it vital that a DDP system itself not be able to send data outside the vehicle, it is equally important that a DDP system be isolated from any other computer systems in vehicles (at least those that are not themselves completely isolated from any telematics functions, if there are any such systems), since those systems are subject to the car manufacturers' unethical privacy practices. We realize that this could limit the available inputs into a DDP system, but such is the consequence of illegitimate privacy practices; the government can either require that the automakers stop engaging in these practices, or it will have to work around them if it wants to create a DDP system that is not privacy-invasive.

If data flows outside the vehicle, protecting privacy becomes far more complex and difficult, and thus uncertain. It raises questions such as what data leaves the car, to whom it goes, and whether that data is truly anonymized or in fact re-identifiable. (One of the findings of data science in recent years is that truly anonymizing data such that it cannot be re-identified is a surprisingly difficult task.[18]) It reduces the privacy protections that come from technological architecture, which would make such a privacy invasion impossible, and increases the importance of *policy* protections, which people must then have faith are being complied with and enforced. That faith can be especially hard to sustain given how hard it is to detect many abuses of personal data.

Building Internet connectivity into a DDP system also opens up such systems to cyber-vulnerabilities. We've seen automotive computing equipment fail time and time again in the face

---

https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/.

[17] *See e.g.*, "Chairwoman Rosenworcel, FCC Chairwoman Calls on Agency to Help Stop Abusers From Using Connected Cars to Harass and Intimidate Their Partners," FCC (Feb. 28, 2024), https://docs.fcc.gov/public/attachments/DOC-400812A1.pdf.

[18] Rob Mitchum, "Common deidentification methods don't fully protect data privacy, study finds," *UChicago News* (Oct. 7, 2022), https://news.uchicago.edu/story/common-deidentification-methods-dont-fully-protect-data-privacy-study-finds.

of adversarial attacks, whether through Internet connectivity or otherwise.[19] There is little reason to think a DDP system would be more robust. Including Internet connectivity merely increases the attack surface against a sensitive component.

If the NHTSA wishes to maximize public acceptance of drunk driving prevention technology, it should also impose privacy regulations on automobile manufacturers to ban their existing illegitimate data collection practices. In addition to being in the public interest, and the fact that these practices greatly complicate the task of building a privacy-protective DDP system, the gradual but inevitable growth of public awareness of those abusive practices is likely to spill over into public distrust of a DDP, even if such a system is properly insulated from the spying technology currently installed in cars.

Accuracy measurement is not a valid reason to transmit sensitive data beyond the car.

Some may want to build a DDP system that permits redistribution of data for the legitimate aim of measuring the accuracy of those systems. Testing the accuracy and efficacy of the technology is an important goal, but there are several reasons why that consideration should not and need not justify the absence of a data-localization requirement.

In addition to the basic functionality of a system, such as whether it reliably separates the driver's breath from their perhaps drunken passengers, it will be important to measure whether a DDP system exhibits differential levels of accuracy by race, gender, disability, or other

[19] Andy Greenberg, "Hackers Remotely Kill a Jeep on the Highway—With Me in It," *Wired* (Jul. 21, 2015), https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/; Kevin Poulsen, "Hacker Disables More Than 100 Cars Remotely," *Wired* (Mar. 17, 2010), https://www.wired.com/2010/03/hacker-bricks-cars/; Rebekah Riess & Peter Valdes-Dapena, "Easily stolen Hyundais and Kias should be recalled, more than a dozen attorneys general say," *CNN* (Apr. 21, 2023), https://www.cnn.com/2023/04/21/business/hyundai-kia-theft-recall-demand/index.html.

characteristics. For example, measuring blood alcohol saturation by looking through the skin could have lower accuracy for people with dark skin, as has been found with pulse oximeters.[20]

But testing and feedback on the accuracy of a DDP system need not involve the collection of data from all systems. It may be possible to create a system that is accurate enough just based on lab testing. If field data is deemed vital enough to warrant an ongoing feedback program, only a sample is needed. Sampling is used across a wide variety of areas from television ratings to political polling to marketing research, and the marginal increase in accuracy produced by scaling up the size of a sample size typically becomes very small and not proportional to the added cost of collecting data from more people. Here that cost should be seen as including loss of privacy and the resulting distrust. A sample group can be drawn from volunteers who agree to data collection based on genuine, meaningful informed consent.

When it comes to detecting false positives (when the DDP tech thinks a person is drunk even when they are not), NHTSA could provide a way for people to voluntarily notify the agency when their DDP system has falsely tripped. That could allow for good-enough tracking of false-positive rates, which is likely to be one of the most important metrics when it comes to consumer acceptance of the technology.

When it comes to false negatives (when the DDP tech fails to detect that a person is drunk), which are less important for public acceptance but more important for safety, that will likely be a much harder figure to track outside of formal tests because, short of a police stop or an accident, false negatives are not likely to come to light. This could be one other advantage of basing any ongoing accuracy measurement program on volunteers, who might be willing, with proper

[20] Anil Oza et al., "COVID-19 made pulse oximeters ubiquitous. Engineers are fixing their racial bias," NPR (Feb. 13, 2023), https://www.npr.org/2023/02/10/1156166554/covid-19-pulse-oximeters-racial-bias; Michael W. Sjoding et al., "Correspondence: Racial Bias in Pulse Oximetry Measurement," 383 *N. Engl. J. Med.* 2477 (Dec. 17, 2020), https://www.nejm.org/doi/full/10.1056/NEJMc2029240.

protections, to participate in the collection of such a ground truth using a separate, more reliable measurement.

3. A drunk driving prevention system must be transparent

Given the constant incentive and temptation to use data that is gathered strictly for safety purposes toward other, often profitable ends, drivers must be able to trust that a DDP system that captures physiological or other sensitive data about them in their car is not engaged in secret data collection or sharing or other illegitimate activities. The only way that can happen is with transparency.

First, the software and physical design of such a system must be visible to any member of the public with the requisite expertise to inspect them and verify that no data is leaving the car, and that the system is otherwise operating as expected. Again, the Volkswagen emissions scandal is a reminder of how hidden code can be programmed to perform secret, unethical operations. Years of experience has also proven that visible source code gives the public opportunities to report bugs that would not otherwise be possible.

Second, data about the technology's accuracy and efficacy rates should be made public so that experts, policymakers, and the general public can evaluate how effective the technology is and judge that against any potential negative side-effects that it may bring. That has been an enormous and scandalous failure with regards to law enforcement breathalyzers, which appear to be leading to false convictions and tragic disruptions of many thousands of innocent people's lives.[21]

[21] Stacey Cowley & Jessica Silver-Greenberg, "These Machines Can Put You in Jail. Don't Trust Them," *New York Times* (Nov. 3, 2019), https://www.nytimes.com/2019/11/03/business/drunk-driving-breathalyzer.html.

Third, any discriminatory impacts should be disclosed, including impacts on people with disabilities such as diabetes, which can produce acetone in a person's breath which registers as ethyl alcohol in a breathalyzer, or impacts on people whose vehicles have been modified due to disability.

III. Some technologies raise more privacy issues than others

NHTSA should assess the privacy implications of different DDP technologies that may be proposed, developed, or adopted. A blood alcohol measurement that is taken from the driver's breath or through skin sensors would collect physiological data (depending on its design, potentially including data other than blood alcohol level). Such data is inherently sensitive but, if collected in accordance with the above principles, need not significantly endanger privacy.

The use of video analytics in an attempt to detect impaired drivers, on the other hand, would require the mandatory presence and activation of a driver-facing camera in each vehicle, which could collect a lot of sensitive information far beyond the driver's level of impairment — not only details such as the driver's demographic characteristics, facial image, eye movements, and behavior patterns, but also potentially the details and activities of others in the vehicle.

The approach of using a driver monitoring system may also rely on the long-term storage of data about each driver, so that their current behavior can be measured against a personal baseline. Insofar as such a system incorporated driving behavior such as steering, braking, and acceleration, it would also likely need to be plugged in to the existing vehicle computer systems — which would be highly problematic since we know those systems are already subject to unethical surveillance by automakers.

Given the fact that video analytics and driving-behavior monitoring systems raise privacy issues that are much more difficult to address, and given what we know about video analytics and its pitfalls, we strongly suspect that a locally calculated, computationally isolated blood alcohol measurement would be the preferable technology from a privacy point of view.[22] A final assessment, of course, would need to be based on the details of a particular technological system or set of standards that is proposed.

Signed,

Jay Stanley
Senior Policy Analyst
ACLU

Jake Wiener
Counsel, Project on Surveillance Oversight
Electronic Privacy Information Center

Lee Tien
Legislative Director and Adams Chair for Internet Rights
Electronic Frontier Foundation

[22] *See* Jay Stanley, "The Dawn of Robot Surveillance: AI, Video Analytics, and Privacy," ACLU (Jun. 17, 2019), https://www.aclu.org/wp-content/uploads/publications/061819-robot_surveillance.pdf.