CA(R)VEAT EMPTOR: CROWDSOURCING DATA TO CHALLENGE THE TESTIMONY OF IN-CAR TECHNOLOGY

Gless, Sabine [1] ; Di, Xuan [2] ; Silverman, Emily [3] [1] University of Basel, Switzerland [2] Columbia University, U.S.A. [3] Max Planck Institute for the Study of Crime, Security and Law, Freiburg/Breisgau, Germany.

ABSTRACT (ENGLISH)

This Article addresses the situation in which a car acts as a witness against its human driver in a court of law. This possibility has become a reality due to technology embedded in modern-day vehicles that captures data prior to a crash event. The authors contend that it is becoming increasingly difficult for drivers to defend themselves in a meaningful way against the testimony of cars and suggest that crowdsourcing data could be a viable option for assessing the trustworthiness of such evidence. The Article further explores whether crowdsourced data could be used as an additional source of information in the fact-finding process and if such data could provide a counterbalance to the prevailing tendency to fault human drivers rather than their vehicles or the manufactures of their vehicles. The practical importance of this issue in the age of driving automation is highlighted, and lawyers, judges, and lawmakers are urged to remain open-minded regarding the use of this new strategy.

FULL TEXT

Headnote

ABSTRACT: This Article addresses the situation in which a car acts as a witness against its human driver in a court of law. This possibility has become a reality due to technology embedded in modern-day vehicles that captures data prior to a crash event. The authors contend that it is becoming increasingly difficult for drivers to defend themselves in a meaningful way against the testimony of cars and suggest that crowdsourcing data could be a viable option for assessing the trustworthiness of such evidence. The Article further explores whether crowdsourced data could be used as an additional source of information in the fact-finding process and if such data could provide a counterbalance to the prevailing tendency to fault human drivers rather than their vehicles or the manufactures of their vehicles. The practical importance of this issue in the age of driving automation is highlighted, and lawyers, judges, and lawmakers are urged to remain open-minded regarding the use of this new strategy.

I.RATTED OUT BY YOUR OWN CAR

In 2015, a Swiss prosecutor brought charges against a driver whose car collided with a motor scooter, causing serious injuries to the rider of the scooter.1 The driver of the car, who was allegedly fatigued at the time of the accident, was charged with driving while unfit to operate a motor vehicle,2 a crime pursuant to the Swiss Road Traffic Act.3 In bringing the charges, the prosecutor relied on both the car's drowsiness detection assistant, which had alerted the driver several times of suspected drowsiness, and its lane-keeping assistant, which had self-activated.4 While the driver eventually accepted a summary penalty order,5 publicly claiming that he was suffering from an as yet undiagnosed sleep apnea at the time of the accident, media coverage did not report on whether or how he defended himself against the declarations of his car.6

The Swiss case introduced here is only one example of a human driver of an automated or partially automated vehicle involved in an accident being charged with a crime. Indeed, a recent U.S. case in which such a vehicle was involved in a fatal accident has received a great deal of media attention.7 The accident, a 2018 crash in Arizona,8 involved a fully autonomous Uber vehicle (Level 4/5)9 that was being tested on public roads with a human backup driver on board. The vehicle struck and killed a pedestrian, and the human driver- who was hired to observe the performance of the vehicle and, if necessary, to take control from the Uber driving system-has been charged with negligent homicide.10 This prominent case is distinguishable from the Swiss case, however, because (according to the information available to the public) the Uber prosecution relies heavily on video footage of the human driver taken by a dashcam and not on assessments conducted by embedded robots of the driver's fitness to control a vehicle.11

This Article specifically addresses the situation of human drivers facing the risk of their cars evaluating their performance and subsequently acting as witnesses against them. It suggests that drivers, currently unable to defend themselves in a meaningful way against such testimony, could turn to crowdsourcing data in the future. The Article begins with an overview of the high-tech accessories that enable cars to observe and record the actions taken by their drivers.12 The underlying technology and associated pitfalls are examined, and the consequences of the absence of pertinent rules in today's procedural codes13 that would enable the successful incorporation of such evidence in the fact-finding stage of criminal cases are discussed. In a next step, the Article explores how to move beyond a car's perspective of an accident: it asks whether, by drawing on crowdsourced data, a "bird's eye" view could be established that would facilitate the testing of the prevailing ground-or "frog's eye"-view constructed by the technology embedded in a vehicle. The Article concludes with a discussion of the need to develop new methods of fact-finding in criminal courts.

II.THE FROG'S EYE VIEW: DATA GATHERED BY A CAR INVOLVED IN A CRASH EVENT

Today's cars gather a plethora of data,14 and in so doing, they create a pool of information that can potentially serve as forensic evidence in a court of law.

A.Sources of Car Data and Their Potential Drawbacks

Data gathered by a car involved in a crash event often provide an overly narrow view of an event, and they are inevitably shaped by the particular technology embedded in that vehicle. Prime examples of such technology include event data recorders (EDRs) and data storage systems for automated driving (DSSADs).

1.Event Data Recorders (EDRs)

EDR technology has been around since the 1990s and was developed to document specific pre-crash data for forensic use.15 This technology offers a limited frog's eye view-or point of view from the ground-of accident-related events, as it captures selected data points a few seconds before an accident occurs.16 Event data recordings can be triggered, for instance, by electronic sensors in the engine, sudden changes in wheel speed, the opening of an airbag, or by the action of a seatbelt, any one of which can arise in connection with an accident.17 Information recorded by an EDR can be collected after a crash and analyzed to help determine what a vehicle was doing before, during, and after the event in question.18

In the United States, where this technology is installed in almost all light vehicles sold,19 it must meet the standards set out in the U.S. Code of Federal Regulations.20 This legal harmonization is, in principle, good news for factfinding in a court of law. The data recorded in an EDR are standardized and can be retrieved using a vehicle interface device.21 EDR recordings can also be authenticated, encrypted, and saved in either untranslated (binary EDR record) or translated (readable to humans) format.22 But EDR data do not provide a comprehensive picture of an accident because EDRs record only a few seconds of pre-event data and can only register two events.23 If a third event occurs, a preceding event will be overwritten. As things stand today, EDRs do not record warnings issued by driving assistants. Consequently, they are rather poor observers with a very limited memory, and they cannot provide a full picture of the myriad factors leading to a particular accident.24 Therefore, if introduced as evidence in a criminal trial, the data retrieved from EDRs yield at best indirect support for (or against) a particular claim concerning a driver's performance.

2.Data Storage Systems for Automated Driving (DSSADs)

Data Storage Systems for Automated Driving are based on advanced in-car data recording technology designed to monitor closely the journey of a vehicle engaged in driving automation. To fully capture the significance of using

DSSADs for evidentiary purposes, it is necessary to understand how humans and automated driver assistance systems (ADASs) share driving tasks and how DSSADs observe and record human conduct.

a. Monitoring Driving with Automated Driver Assistance Systems (ADASs)

Today's cars make driving more convenient by means of embedded ADASs capable of emergency braking,25 speed assistance,26 lane keeping,27 detecting drowsiness in the human driver,28 and detecting pedestrians on the street.29 These assistants are essentially robots capable of sensing their environment, collecting and processing data, and reacting autonomously on the basis of their evaluation of safety-relevant driving situations.30 Currently, a number of car models are equipped with such systems, and ADAS installation in newly built vehicles sold in the European Union became mandatory in 2022.31 Their use raises a number of expectations, including hope for improved road safety due to their ability to warn human drivers of impending danger, to help human drivers navigate standard traffic situations, and to notify them to take over after a period of fully automated driving.32 Because ADASs make a record of every alert they issue, they also seem poised to create a whole new category of forensic evidence.33 One prominent example of such a robot, and the system that is the focus of the rest of the Article, is a car's drowsiness detection assistant.34

If, as in the introductory example, an accident takes place after drowsiness alerts have been issued, the stored record of these alerts could function as a kind of robot testimony.35 It could serve as evidence that the human driver involved in the accident was on notice of his or her unfitness-or even as proof of the driver's actual unfitness to operate a vehicle. Thus, a robot's observations could play a pivotal role in the fact-finding stage of an ensuing criminal case, should a standard for such technology be developed.

b. Building Robot Testimony

To understand the implications of robot testimony and its pros and cons (in particular, bias, risks to privacy, and the consequences of the lack of common standards), it is necessary to look more closely at the components of the driving assistants that feed information into a particular DSSAD. From a technological perspective, drowsiness detection assistants can be divided into three main categories-vehicular, behavioral, and physiological-depending upon the techniques they employ.36 All of the techniques use machine learning and each of them works differently.37 Of particular interest in the legal context is the fact that each technique records different kinds of data. Thus, the choice of which technique to employ is crucial from an evidentiary point of view, as the way it works and the data it stores set the stage for the creation of car testimony and determine the resulting degrees of accuracy and invasiveness.

Vehicular-based techniques look for patterns of frequent lane changing, variation in steering wheel angles or driver grip, and anomalies in lane departure, speed, and acceleration.38 Behavioral-based techniques measure fatigue by means of driver eye movement, facial expressions, and yawning and require methodological development to classify facial changes from camera images or video streams.39 Techniques based on physiological parameters detect drowsiness based on drivers' physical conditions, such as heart rate, respiratory rate, and body temperature. These biological parameters promise more reliability and accuracy in drowsiness detection as they deal with direct physical changes in the driver. Measuring them, however, is an invasive process and could, in some instances, require electrodes to be placed directly on a driver's body.40 The choice of which technology to employ is left entirely up to the respective car manufacturer, automotive supplier, or programmer.41

In the case of drowsiness detection assistants, engineers who determine the required quantity and type of machine learning shape the driving assistant's ability to observe, record, and give information regarding the human driver's conduct; furthermore, machine-learning datasets introduce a number of possible sources of error, including training data bias, labeling bias, and algorithm bias.42 Training data bias includes imbalanced datasets that are collected primarily from a particular population group and may not generalize well to generic populations.43 When training drowsiness detection assistants, engineers have to face the so-called "white guy problem,"44 as, for instance, aging female drivers with drooping eyelids, those who drive in a more relaxed sitting position, and most non-Caucasian faces may not fit into the training pattern. In addition, training algorithms themselves can lead to biased predictions in a test dataset due to a lack of transparency concerning the way the algorithm operates45 (referred to as the black box issue46). Consistent with the variation in the underlying technology, each category of drowsiness detection assistants stores data according to its own parameters of measuring driver fatigue-and thus runs the risks of specific errors.

Although driving assistants became mandatory in Europe in January 2022,47 the types of data that must be recorded have not yet been identified. Thus, the information recorded may vary widely, and without clear standards for data generation and data recording, each technique offers its own blend of accuracy and invasiveness. Ultimately, car manufacturers and automotive suppliers make trade-offs that shape the evidentiary value of car testimony. This is one of the reasons for the push to establish uniform DSSAD requirements or to extend the capabilities of EDRs and thereby to standardize a car's "memory" of events.48 A number of groups at both the domestic49 and the international50 level are preparing for the adoption of common standards.51 In particular, the World Forum for Harmonization of Vehicle Regulations,52 a working group under the aegis of the United Nations Economic Commission for Europe (UNECE), is working on streamlining rules for automated driving and for standards regarding the availability and accessibility of data.53 Until now, the absence of such standards has impeded the accessibility, retrievability, and reproducibility of data and undermined any overall guarantee of a verifiable record of what happened in the run-up to an incident.

Given continued technological development54 and ongoing political impetus, it seems likely that, in the coming years, in-car technology will be capable of continuous storage of the data generated and recorded during automated car trips.55 This includes timestamps, activation and deactivation of an automated driving assistant, the reason for deactivation (i.e., override by human driver), take-over requests from driving assistants to human drivers, and drowsiness detection alerts (of particular interest here as they are the kind of warning implicated in the Swiss prosecution of a driver discussed in Part I). Of course, such data can also be used in defense of a human driver standing trial following an accident. The goal should be for the stored data to be accessible via a standard interface that is shielded from corruption.

3.Additional Car Data

After an accident, it may be possible to retrieve additional data that has been stored in-car.56 Indeed, contemporary vehicles may broaden their frog's-eye view by recording a great deal more forensic information than consumers (or forensic experts) know is being stored.57 In addition to crash event data, for example, Tesla vehicles record driving data including speed, accelerator pedal position, steering wheel angle, brake usage, forward camera footage and crash event data.58 These detailed bits of information, referred to as naturalistic driving data,59 include data on the driver, the vehicle, and the environment and are collected via passive or unobtrusive data-recording technologies (e.g., in-vehicle data-recording devices, sensors, and cameras) during routine driving trips. In addition, some smart vehicles also download data from a user's smartphone, including contact lists, emails, and phone call logs, whenever the device is connected to the car's infotainment system.60 In theory, all of this data could be harvested for fact-finding purposes-specifically, for instance, to validate or challenge a particular driving assistant's testimony. In practice, however, such data are generated and recorded in many different ways, and stakeholders in criminal justice proceedings are faced with a number of hurdles, including access (in particular, retrievability and encryption), barriers designed to protect user privacy (unwillingness to release sensitive data such as in-vehicle camera footage or location histories of a particular driver), and problems related to evidentiary value (lack of standards governing the digital investigation of a vehicle).61

4.Summary

In-car technology can provide important information concerning the circumstances of an accident. But this technology offers only a frog's-eye perspective-or point of view from the ground-which has inherent limitations. Even if investigators in the Swiss introductory example had access to all available car data, it might still have been unclear whose testimony (the human driver's or the driving assistant's) ought to be trusted. Unlike the simple EDRs in use in the United States, DSSADs promoted in Europe will be capable of collecting detailed driving data continuously. The goal is for that data to be available to show what occurred before and during an accident and to shed light on an individual's typical driving behavior. While DSSAD information can reveal abnormal driving patterns, it is certainly not a one-to-one mapping of reality; rather, it is a series of limited observations undertaken by in-car technology. As well as concerns about accuracy, the collection of car data raises privacy issues. With such data, for example, individual drivers can be identified, their movements traced, and other threats to privacy created.62 Data stored in EDRs, in comparison, generally pose less of a challenge to privacy, but they provide limited, event-triggered data that may not suffice to reconstruct an accident. Whichever route is chosen, appropriate regulations governing the recording and storage of specific data in a specific form will serve to standardize a car's capacity for observation, assessment, and memory. Without standards, decisions concerning which data are recorded and how they can be retrieved remain within the discretion of programmers and manufacturers. Consequently, the set of data available may be seen to be one-sided or even unreliable-and its introduction as evidence in a criminal court problematic.

B. Absence of Pertinent Rules of Criminal Procedure Governing the Admissibility of In-Car Data

If in-car data are deemed admissible as evidence in criminal court, a number of new legal issues arise in addition to the inability of in-car technology-robot testimony in particular63-to provide sufficient information concerning the circumstances of an accident.64 These issues include the conditions under which prosecutors and defense counsel should be permitted to tap into this newly emerging pool of "evaluative data,"65 how judges should allow a car's testimony to be presented in a criminal trial, and what avenues of defense should be available to those who wish to challenge such testimony.66 These questions are difficult to answer, due, at least in part, to the absence of pertinent rules of criminal procedure.

Today ' s rules of criminal procedure are tailored to an analog world in which various categories of evidence have been tested and evaluated by humans for centuries. Human witnesses are confronted by the parties; exhibits are examined by the parties; and forensic evidence is explained by experts. In contrast, evaluative data generated by driving assistants are routinely derived from black box machine-learning models and complex algorithmic operations, and the entity behind these operations (the robot that senses, processes, and evaluates information before recording its assessment) cannot be summoned to the witness stand or otherwise vetted.67 Furthermore, a drowsiness detection assistant may combine input from the sensors of various other driving assistants (e.g., lanekeeping assistants) with the human driver's steering movements, eyelid movements, and sitting position68 in such a way that no human being could understand why a drowsiness alert was triggered. Thus, it is virtually impossible for human beings to completely explain and examine in a criminal court the digital layer of intelligence added by such robots.

This issue highlights a significant drawback of this new form of testimony-namely, the lack of tools with which it can be challenged if proffered as evidence in a criminal proceeding.69 In this regard, it is distinguishable from other forms of testimony for which various evidentiary procedures have developed over the years. For instance, if calculations performed by computers operating without the assistance of machine learning technology are introduced as substantive evidence in the United States, they must be authenticated, typically by showing, pursuant to Rule 901(b)(9) of the Federal Rules of Evidence, that they were created by a process or system that produces accurate results.70 European courts have adopted a variety of different approaches, but all are prohibited by the European Court of Human Rights from admitting evidence that fails to satisfy a minimum standard of reliability; to ensure that the standard is met, these courts often rely on the stakeholders in a criminal proceeding to vet the proffered evidence by exercising their confrontation rights.71 In Germany, for example, the defense must be granted access to relevant measurement data to ensure meaningful vetting of the results of a radar gun in speeding cases.72 Access to this information can help reveal whether a series of measurements can be considered reliable.73 Furthermore, if the defense wishes to cast doubt on an expert's findings and to offer an independent proposition regarding the results of the radar gun, the court can require law enforcement authorities to submit a second data set based on an independent measurement method, such as a videotaping of the radar gun's measurement and its environment.74 By providing data external to the car, results can be verified independently.

III.THE BIRD'S EYE VIEW: A WAY TO CHALLENGE IN-CAR DATA

The question arises as to whether it is necessary to move beyond the frog's eye view of traffic accidents provided by in-car data in order to achieve a fair fact-finding process. The underlying rationale is that in a criminal trial, human drivers not only have the right to challenge statements made by human witnesses but must be able to defend themselves against in-car data, including robot testimony generated by driving assistants. Crowdsourced videos or images of an accident could fill this gap. Indeed, a defendant's best chance to mount a meaningful defense might be to adopt this type of bird's eye view.

A. Crowdsourced Data: A Path to Better Fact-Finding

Crowdsourcing data, a method of forming a dataset using significant amounts of information provided by an undefined (and generally large) network of people,75 appears to be a promising way of establishing a counternarrative regarding the circumstances surrounding an accident.

1. Crowdsourcing Based on Platforms

Crowdsourcing data concerning an accident are in line with the broader approach of outsourcing tasks to a large group rather than assigning them to a single entity.76 Thanks to information technology and social media, crowdsourcing has become common in many areas and has contributed to both innovation77 and scientific research.78 As a rule, crowdsourced data are cheap and convenient, and they can be expected to deliver a more objective perspective than one (or even several) traditional human witnesses.79

Furthermore, crowdsourcing data in the context of crash events can be linked to existing practices as crowdsourcing is already used to analyze road accidents and to warn drivers. One example is the traffic app Waze,80 a popular crowdsourced navigation platform with 130 million monthly users.81 Waze provides turn-by-turn real-time navigation instructions and also supports a shared platform where users can submit updated road and traffic information and report incidents or accidents.82 As Waze crowdsources community navigation experiences for up-to-date information and alerts, the reports have been leveraged for crash analyses83 and have been found to be positively correlated with crash risk and police accident reports.84 It seems that data from Waze crash alerts detect motor vehicle crashes faster than the corresponding police reports and thus can be leveraged for crash prediction.85 Consequently, in traffic engineering, there has been growing interest in recent years in asking private persons to contribute to traffic data collection, traffic information reporting and analysis, and traffic relief proposals.86

2. Crowdsourcing Based on Data from Connected Cars

Aggregating crowdsourced data from several cars could provide another counternarrative to the frog's-eye view. Both connected87 and automated vehicles are outfitted with numerous sensors, including cellular vehicle-to-everything (C-V2X)88 communication and dedicated short range communication (DSRC)89 devices, forward and rear cameras, and Lidars (light detection and ranging sensors), all of which could be crowdsourced to reconstruct a crash scene from a bird's eye view.90 If C-V2X and DSRC communication devices become prevalent (a development that the U.S. Department of Transportation has been pushing since 201691), they will collect billions of data points from cars92 that could potentially be used as crowdsourced testimony. For example, neighboring connected vehicles and infrastructure could receive basic safety messages from a subject vehicle, including its location, speed, acceleration, and timestamps. Aggregating this information for the vehicle in question from surrounding vehicles could help reconstruct its driving trajectories.

B. Pitfalls of Crowdsourced Data

Of course, using crowdsourced data is not an entirely new concept. Law enforcement agents have always relied on the statements of eye witnesses and tips from the community to build their cases. But using data collected by equipment that monitors private and public areas is a different matter, and one that, aside from offering the potential advantages discussed above, presents challenges of its own. First, information provided from private citizens (such as that derived from Waze or other platforms) can be hacked and spoofed, which threatens its reliability.93 Second, the process of gathering privately collected information may be unclear or subject to intellectual property restrictions (e.g., source code).94 Third, platforms and data sources that can be leveraged for citizen forensics may threaten privacy interests, as they might expose daily movements, habits, or protected religious or political activities.95 At this point, it is impossible to provide a one-size-fits-all solution to the aforementioned risks. From a legal standpoint, solutions will vary widely from jurisdiction to jurisdiction. For example, installing a dashboard camera on a car's windshield is legal in some European countries but illegal in others96 with a similar lack of consistency in the United

States.97 The precariousness of the legal situation is exacerbated when footage of individuals and images of their faces or license plates from public streets are gathered indiscriminately. The circumstances under which dashboard camera footage harvested from private cars can be used as evidence in a criminal trial will have to be determined on a case-by-case basis. If footage from a dashboard camera or of a situation like the one described in Part I is used in a criminal proceeding, what information can be reliably gained from it? If other cars had captured images showing the motor scooter running a red light, could the pictures be used to prove the innocence of the driver of the car? On the other hand, if nearby cars or surveillance cameras recorded data indicating that the car was being driven erratically, could this information be used against its driver? Furthermore, how can it be ensured that the recordings have not been tampered with?

These questions illustrate the multitude of technical and legal questions that will have to be addressed. For instance, to meet legal standards for evidentiary reliability, it might be useful to define a new type of chain of custody for crowdsourced data or to require authentication and additional checks for reliability in the relevant jurisdiction. To a certain degree, this issue of data reliability98 might be addressed with new technologies such as blockchain technology,99 which can ensure a certain degree of reliability.100 A potential application of this technology in the context of vehicular digital forensics is the following:101After a crash event, the competent law enforcement agency asks the court for a warrant to collect relevant accident data. The court issues a warrant, signed by an encrypted key, to the law enforcement agency. The agency decrypts the key and collects the data that could be leveraged for criminal proceedings. During the investigative process, the blockchain is maintained by the court and the law enforcement agencies to ensure validity and legitimacy. Then a background program in the vehicle-a so-called forensic daemon102-verifies the validity of the data collection request from the law enforcement agency and uploads vehicle data to the blockchain and data storage nodes.

As blockchain technology becomes more advanced and more widely accepted by car manufacturers, social media platforms, and cellphone hardware and service providers, a channel could potentially open for conversation between law enforcement and data providers about how the pitfalls of crowdsourcing can be addressed in a way that would benefit fact-finding.

C.Crowdsourcing Data as a New Defense Strategy

If the most urgent problems of crowdsourcing data could be overcome, it could offer a new strategy for trial participants seeking to challenge in-car data.103 Defense lawyers, in particular, might be interested in using crowdsourced data to vet in-car testimony presented by a prosecutor as evidence. Should lawyers opt for crowdsourcing, a network of defense counsel could provide a portal where private individuals could leverage their digital devices for recovery, investigation, examination, and analysis based on things like dashboard camera recordings, photos, social media content, CCTV camera footage, traffic surveillance camera footage, vehicle maintenance records, and the drivers' records.104 Since this kind of crowdsourced data portal does not yet exist, researchers and law enforcement agencies should collaborate to develop a crime data management portal that builds on blockchain technology to ensure that data collected from the various devices are not tampered with and that privacy is preserved.

At first glance, crowdsourcing appears to be an obvious defense strategy, given that human drivers appear to be at a disadvantage since a car's capacity for recollection (and thus the basis for its potential testimony) is shaped by car manufacturers, auto suppliers, and programmers. The interests of these entities may differ vastly from those of human defendants due to potential product liability that could make such entities fallback defendants. This seems particularly true of data generated during automated driving, for instance, by drowsiness detection assistants. It is important to note that in-car data and crowdsourced data can work both for and against the defense. In fact, crowdsourcing has proven an efficient tool for inquiries in various areas, bringing together individuals, NGOs, and industry.105

Creating a bird's eye view with the help of crowdsourced data in a particular case could be beneficial to the goal of finding the truth and could shift the focus away from individual defendants. Crowdsourcing might be one way to prepare a coherent fact-finding process in the era of smart products. In other words, as the Internet of Things becomes increasingly mainstream, it may turn into a quasi-ubiquitous potential witness-one whose testimony could be used to challenge information provided by in-car data and more specifically to the testimony of driving assistants.

IV.NEW PROSPECTS FOR FINDING THE TRUTH

Public acceptance of a criminal verdict depends, to a great extent, on the perception that the conviction (or acquittal) reflects the truth about what happened during the incident at issue. Thus, when the question of guilt or innocence in a criminal proceeding turns on the determination of the events occurring during the lead-up to a crash, lawyers and other court actors must be open to new methods of fact-finding.

In many ways, data crowdsourcing is in line with the modern day Zeitgeist of fact-finding and has proven its aptitude: Social media data is increasingly leveraged as a support tool to enhance situational awareness on public roads, including monitoring, crisis management, and intelligence gathering.106 For example, following the Boston Marathon bombing in April 2013, the Boston Police Department used data from Twitter to collect information, identify suspects, and communicate to the public.107 Investigators have also harvested evidence from social media for use in prosecuting participants in the January 6, 2021 insurrection at the U.S. Capitol.108 A type of crowdsourcing check that would ask internet users to help assess and verify publicly available information using other corroborative information could be developed. For instance, in the case of Gabrielle Petito, who went missing in the United States in the summer of 2021, many TikTok, Instagram, Twitter, and YouTube users uploaded videos they thought might help locate Gabrielle, and many individuals chipped in to help analyze those videos.109

As a rule, criminal courts are reluctant to avail themselves of new methods, and all parties must contribute to the development of data sources and reliability testing.110 As things stand today, in-car data (and the testimony of driving assistants, in particular) will likely be proffered as evidence in the future. Lawyers face a number of challenges, as criminal justice systems do not yet have the tools with which to engage in meaningful vetting of the validity of such testimony. Crowdsourced data appear to be one of the few viable options for testing its trustworthiness, but their admission would require the adoption of significant changes to evidentiary proceedings-and might also require the augmentation of courtroom technological capabilities.111 Not only will procedural codes need to be overhauled, but our thinking and overall approach will have to be amended as well. The Swiss example from Part I illustrates why human drivers need an effective means of building a counternarrative to car testimony. It is our task to search for data that can provide a bird's eye view, thereby rescuing human drivers from the potentially dangerous situation of a frog on the road, namely, a creature that fails to see important information due to its own limited perspective.

Sidebar

CITATION: Sabine Gless, Xuan Di, &Emily Silverman, Ca(r)veat Emptor: Crowdsourcing Data to Challenge the Testimony of In-Car Technology, 62 Jurimetrics J. 285-302 (2022).

This Article is the result of a cooperation under the umbrella of a research group at the Center of Interdisciplinary Studies at the University of Bielefeld (https://www.uni-bielefeld.de/(en)/ZiF/ FG/2021SmartProducts/index.html). We are grateful for this support and for the ongoing funding from the Swiss National Science Foundation. For research into legal challenges arising from humanrobot interactions, go to https://snf.ch/en/FKhU9kAtfXx7w9AI/page/home.

Footnote

1. Swiss Politician Fined Over Crash That Injured 17-Year-Old, Local (Oct. 31, 2016, 11:31 AM), https://www.thelocal.ch/20161031/swiss-politician-fined-over-crash-that-injured-17-year-old/ [https://perma.cc/TYW4-RU6X].

2. See id.

3. Strassenverkehrsgesetz [SVG] [Road Traffic Act] Dec. 19, 1958, SR 741.01, art. 91, para. 2 (Switz.) (status of Jan. 1, 2020).

4. See Swiss Politician Fined Over Crash That Injured 17-Year-Old, supra note 1.

5. A summary penalty order is an order issued by the public prosecutor for a criminal offense that fixes, without trial, a penalty that will become a final and enforceable criminal judgment unless the accused requests within the statutory period that the matter be dealt with under the normal trial mode. For additional details, see Schweizerische

Strafprozessordnung [StPO] [Code of Criminal Procedure] Oct. 2007, SR 312, arts. 352-356 (Switz.) (status of July 1, 2022); see Swiss Politician Fined Over Crash That Injured 17-Year-Old, supra note 1.

6. See Swiss Politician Fined Over Crash That Injured 17-Year-Old, supra note 1.

7. Lauren Smiley, 'I'm the Operator': The Aftermath of a Self-Driving Tragedy, WIRED (Mar. 8, 2022, 6:00 AM), https://www.wired.com/story/uber-self-driving-car-fatal-crash/ [https://perma. cc/Q6YF-A8YQ].

8. Id.

9. For definitions of levels of driving automation, see Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles, Standard J3016 (Soc'y Auto. Eng'rs Apr. 2021) [hereinafter SAE, Standard J3016].

10. Smiley, supra note 7. At the time of publication, the case had not yet gone to trial. A second accident with fatalities that has been reported in the media, a 2019 crash in California, involved a Tesla Model S equipped with a partially automated driving system (Level 2/3). The driver of the Tesla, which ran a red light and crashed into another car, killing its two occupants, has been charged with vehicular manslaughter. Tom Krisher &Stefanie Dazio, Felony Charges Are 1st in a Fatal Crash Involving Autopilot, AP News (Jan. 18, 2022), https://apnews.com/article/tesla-autopilot-fatal-crash-charges-91b4a0341e07244f3fb3051b5c2462ae [<https://web.archive.org/web/20220503161804/https://apnews.com/article/tesla-autopilot-fatal-crash-charges-91b4a0341e07244f3f03051b> 5c2462ae].

11. Smiley, supra note 7. Furthermore, unlike the situation in the Swiss case, the circumstances as reported in the press of the Uber accident, id, and the Tesla accident, Krisher &Dazio, supra note 10, at least suggest the possibility that the automation technology in the respective vehicles failed to function properly, a suggestion that, in turn, raises the question about why no charges were brought in either case against the automobile manufacturers or any of the other parties who contributed to the development of the technology employed by the vehicles in question. See Smiley, supra note 7 ("Uber told the NTSB that its tech had never identified Herzberg as a person. Nearly every time the system changed what it thought Herzberg was-a car, a bike, other-it started from scratch in calculating where the object might be headed, that is, across the road into the Volvo's lane.").

12. The vehicle autonomy levels focused on in this Article are Level 1 (vehicles equipped with driver assistance features) and Level 2 (vehicles equipped with advanced driver assistance features where "Driver Support Systems" assist the human driver in certain scenarios such as cruise control and lane assist). See SAE, Standard J3016, supra note 9.

13. Examples of these types of procedural codes include Germany's Strafprozessordnung (StPO) (Code of Criminal Procedure); Switzerland's Schweizerische Strafprozessordnung (StPO) (Code of Criminal Procedure); and the U.S. Federal Rules of Evidence.

14. See, e.g., Nhien-An Le-Khac et al., Smart Vehicle Forensics: Challenges and Case Study, 109 Future Generation Comput. Sys. 500 (2020).

15. Event Data Recorder, Nat'L HIGHWAY TRAFFIC SAFETY ADMIN., https://www.nhtsa.gov/ research-data/event-data-recorder [https://perma.cc/2MWB-6A8D].

16. See id.

17. See id.

18. See id.

19. For vehicles made in model year 2017, it was 99.6 percent. See 84 Fed. Reg. 2804, 2805 (Feb. 8, 2019).

20. 49 C.F.R. 563.7 (2020).

21. See Surface Vehicle Recommended Practice, Event Data Recorder, Standard J1698 (Soc'y Auto. Eng'rs May 2014) [hereinafter SAE, Standard J1698].

22. Id. 3.12(c)-(d).

23. For further information on the recording of pre-crash data, which generally include vehicle speed, throttle position, and brake activity, see id.

24. See Hampton Gabler et al., Crash Severity: A Comparison of Event Data Recorder Measurements with Accident Reconstruction Estimates (Soc'y Auto. Eng'rs, Technical Paper No. 2004-01-1194, 2004).

25. Lan Yang et al., A Systematic Review of Autonomous Emergency Braking System: Impact Factor, Technology, and Performance Evaluation, 2022 J. ADVANCED Transp., art. no. 1188089, 2022, at 1, 1-2.
26. Margaret Ryan, Intelligent Speed Assistance: A Review of the Literature. A Report Commissioned by the Road Safety Authority (RSA) 6 (2018).
27. Chadaporn Keatmanee et al., Vision-Based Lane Keeping-A Survey, in 2018 International Conference on Embedded Systems and Intelligent Technology &International Conference on Information and Communication Technology for Embedded Systems (ICESIT-ICICTES) 1 (2018), https://ieeexplore.ieee.org/document/8442051 (follow "Download PDF" hyperlink to access PDF).
28. See Muhammad Ramzan et al., A Survey on State-of-the-Art Drowsiness Detection Techniques, 7 IEEE ACCESS 61904 (2019).
29. Walter Eichendorf, Automated Driving Technology Improves Road Safety: Regulation Is Needed, However, Kommission Arbeitsschutz &Normung (Feb. 2020), https://www.kan.de/en/ publications/kanbrief/mobility-in-our-time/automated-driving-technology-improves-road-safetyregul ation-is-needed-however/page [https://perma.cc/ZN3W-JV47].
30. See Ryan Calo, Robotics and the Lessons of Cyberlaw, 103 Calif. L. Rev. 513, 529-31 (2015).
31. 2019 O.J. (L 325) 1.
32. That is, Level 3 or above. See SAE, Standard J3016, supra note 9.
33. See Eoghan Casey, Digital Evidence and Computer Crime 22-26 (3d ed. 2011). For a taxonomy of generations of evidence, see Erin Murphy, Inferences, Arguments, and Second Generation Forensic Evidence, 59 HASTINGS L.J. 1047 (2008).
34. For additional details, see Emily Silverman, Jörg Arnold &Sabine Gless, Robot Testimony? A Taxonomy and Standardized Approach to Evaluative Data in Criminal Proceedings, in Human-Robot Interaction: A Digital Shift in Law and its Narratives (Sabine Gless &Helena Whalen-Bridge eds., forthcoming 2023).
35. For the purposes of this Article, the term robot testimony is defined as the output of a robot that conveys information and implicates credibility. See also Andrea Roth, Machine Testimony, 126 Yale L.J. 1972, 1976 n.11, 2006 (2017).
36. For a detailed summary of each technique, see Ramzan et al., supra note 28, at 61905-14.
37. Id.
38. Id. at 61910-12.
39. Id. at 61906-10.
40. Id. at 61912.
41. See Matej Drha, Identification and Recognition of the Driver's Behavior, in PROCEEDINGS in Informatics and Information Technologies: Student Research Conference 44, 45 (Ján Lang &Rastislav Bencel eds., 2020), http://www2.fiit.stuba.sk/iitsrc/iit-src2020-proceedings. pdf [https://perma.cc/5FG6-NYQA].
42. For example, a labeling bias can occur with reduced understanding by researchers classifying what does and what does not look like a fatigued driver. See Adam Zewe, Can MachineLearning Models Overcome Biased Datasets?, MIT News (Feb. 21, 2022), https://news.mit.edu/ 2022/machine-learning-biased-data-0221 [https://perma.cc/GN74-55TF].
43. Kate Crawford, Artificial Intelligence's White Guy Problem, N.Y. TIMES (June 26, 2016), https://www.nytimes.com/2016/06/26/opinion/sunday/artificial-intelligences-white-guy-problem.html [https://perma.cc/GAK6-NY CM].
44. Id.
45. Vivek Khetan, Bias in Machine Learning Algorithms, MEDIUM (Apr. 6, 2019), https:// towardsdatascience.com/bias-in-machine-learning-algorithms-f36ddc2514c0 [https://perma.cc/34NXJ7D3].
46. Katherine Kwong, The Algorithm Says You Did It: The Use of Black Box, 31 HARV. J.L. &Tech. 275, 291-92 (2017); Stephanie J. Lacambra et al., Opening the Black Box: Defendants' Rights to Confront Forensic Software, Champion, May 2018, at 28, 28-29 (2018).

47. 2019 O.J. (L 325) 1 (providing standards for subsequently installed technology); see also supra Section II.B.2.a.
48. See, e.g., Antwort der Bundesregierung [Response of the Federal Government], Deutscher Bundestag: Drucksachen [BT] 19/16250 (Dec. 30, 2019) (Ger.).
49. See, e.g., id.
50. U.N. Economic Commission for Europe World Forum for Harmonization of Vehicle Regulations, Proposal for a New UN Regulation on Uniform Provisions Concerning the Approval of Vehicles with Regards to Automated Lane Keeping System, ¶¶7-8, U.N. Doc. ECE/TRANS/ WP.29/2020/81 (Apr. 6, 2020).
51. U.N. Economic Commission for Europe World Forum for Harmonization of Vehicle Regulations, Framework Document on Automated/Autonomous Vehicles, U.N. Doc. ECE/TRANS/ WP.29/2019/34 (Apr. 15, 2019), https://unece.org/DAM/trans/doc/2019/wp29/ECE-TRANS-WP 29-2019-34e.pdf [https://perma.cc/2KEF-K6E6].
52. WP.29-Introduction, U.N. Econ. Comm'n for Eur., https://unece.org/wp29-introduction [https://perma.cc/F9TV-X8XW].
53. A framework document on automated/autonomous vehicles prepared by representatives of China, the European Union, Japan, and the United States, see U.N. Economic Commission for Europe, World Forum for Harmonization of Vehicle Regulations, Framework Document on Automated/Autonomous Vehicles (2020), https://unece.org/DAM/trans/doc/2020/wp29grva/FDA V_Brochure.pdf [https://perma.cc/4WAZ-XAUB], was adopted by the World Forum for Harmonization of Vehicle Regulations (WP.29) at its 178th session, see U.N. Economic Commission for Europe World Forum for Harmonization of Vehicle Regulations, Reports of the World Forum for Harmonization of Vehicle Regulations on Its 178th Session, ¶27, U.N. Doc. ECE/TRANS/WP.29/1147 (July 8, 2019), https://unece.org/fileadmin/DAM/trans/doc/2019/wp29/ ECE-TRANS-WP.29-1147e.pdf [https://perma.cc/2Z7G-ALUA].
54. SAE, Standard J1698, supra note 21; see Surface Vehicle Recommended Practice, Heavy Vehicle Event Data Recorder (HVEDR) Standard-Tier 1, Standard J2728 (Soc'y Auto. Eng'rs June 2010) (for a possible starting point for common standards on DSSAD); see also Surface Vehicle Recommended Practice, Pedestrian Protection EDR Output Data Definition, Appendix to SAE J1698-1 Event Data Recorder-Output Data Definition, Standard J1698-1A (Soc'y Auto. Eng'rs Apr. 2021); Surface Vehicle Recommended Practice, Event Data Recorder-Retrieval Tool Protocol, Standard J1698-2 (Soc'y Auto. Eng'rs Jan. 2013); Surface Vehicle Recommended Practice, Event Data Recorder-Compliance Assessment, Standard J1698/3 (Soc'y Auto. Eng'rs June 2013); Surface Vehicle Recommended Practice, Automated Driving System Data Logger, Standard J3197 (Soc'y Auto. Eng'rs July 2021) (defining minimum data element set and common record format).
55. For definitions of levels of driving automation, see SAE, Standard J3016, supra note 9.
56. See Andrew J. Hawkins, Tesla's Driving Data Storage System Hacked by Dutch Investigators, Verge (Oct. 21, 2021, 2:06 PM), https://www.theverge.com/2021/10/21/22738747/ tesla-driving-data-hack-dutch-investigators-autopilot [https://web.archive.org/web/20211103002455/ https://www.theverge.com/2021/10/21/22738747/tesla-driving-data-hack-dutch-investigators-autopilot].
57. See id.
58. Id.
59. Frank Knoefel et al., Naturalistic Driving: A Framework andAdvances in Using Big Data, Geriatrics, June 2018, art. no. 16, at 1, 3.
60. See supra text accompanying note 14.
61. Le-Khac et al., supra note 14, at 502.
62. See Colum. U. Sch. Eng'g &Applied Sci., Where You Go Tells Who You Are-and Vice Versa, Sci. Daily (Nov. 19, 2018), https://www.sciencedaily.com/releases/2018/11/181119155935 .htm [https://perma.cc/9T74-P9WP].
63. See supra text accompanying note 35.
64. Supra Section II.A.3.
65. Silverman et al., supra note 34.
66. Sabine Gless, AI in the Courtroom: A Comparative Analysis of Machine Evidence in Criminal Trials, 51 Geo. J.

Int'L L. 195 (2020).
67. For details, see supra note 34.
68. For details on drowsiness detection technology, see Ramzan et al., supra note 28, at 61905-14.
69. Supra text accompanying note 66.
70. Richard O. Lempert et al., A Modern Approach to Evidence 1326-27 (5th ed. 2013).
71. Trofimov v. Russia, Eur. Ct. H.R., App. No. 1111/02, ¶¶32-33 (2008); Khodorkovskiy &Lebedev v. Russia, Eur. Ct. H.R., App. Nos. 11082/06 &13772/05, ¶700 (2013); Sadak and Others v. Turkey, Eur. Ct. H.R., App. Nos. 29900/96, 29901/96, 29902/96, &29903/96, ¶63, ¶67 (2001); Joelle Vuille et al., Scientific Evidence and the Right to a Fair Trial Under Article 6 ECHR, 16 LAW Probability &Risk 55, 57-58 (2017).
72. BVerfGE, 2 BvR 1616/18, Nov. 12, 2020, https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2020/11/rk20201112_2bvr161618.html [https://perma.cc/RH98BLG4].
73. See id.
74. For the legal standard in Switzerland, see, e.g., Bundesgericht [BGer] [Federal Supreme Court] Jan. 27, 2016, 6B_774/2015, ¶3.3 ("Ein Messmittel muss entweder zwei voneinander unabhängige Messverfahren aufweisen oder es muss ein Mehrfach-Mess-System vorhanden sein, dessen Messwerte anhand einer zeitlich festgelegten Bildserie oder einer definierten FixdistanzBildaufnahme nachträglich rekonstruiert werden können [A measuring device must either have two independent measuring methods or there must be a multiple measuring system, the measured values of which can be reconstructed retrospectively on the basis of a series of images fixed in time or a defined fixed-distance image recording . . . .]").
75. Jeff Howe, Crowdsourcing: A Definition, CROWDSOURCING BLOG (June 2, 2006), https: //crowdsourcing.typepad.com/cs/2006/06/crowdsourcing_a.html [https://perma.cc/3RAU-4YC4]; Crowd-Sourced Data, DIME Wiki, https://dimewiki.worldbank.org/Crowd-sourced_Data#:~:text=is %20well%2Dtested.- ,Overview,given%20its%20relatively%20low%20cost [https://perma.cc/K5DM -JNYJ].
76. See Daren C. Brabham, Crowdsourcing (2013); see also Lateshia Beachum, A White Off-Duty Deputy Says He Shot a Black Man Who Jumped on His Truck, WASH. POST (Jan. 11, 2022), https://www.washingtonpost.com/nation/2022/01/11/jason-walker-/ [https://perma.cc/2PB3-HRFR].
77. See Winfried Ebner et al., Community Engineering for Innovations: The Ideas Competition as a Method to Nurture a Virtual Community for Innovations, 39 R&D Mgmt. 342 (2009).
78. See Future Directions FOR Citizen Science and Public Policy 12 (Katie Cohen &Robert Doubleday eds., 2021), https://www.csap.cam.ac.uk/media/uploads/files/1/foture-directions -for-citizen-science-and-public-policy-web-v6.pdf [https://perma.cc/XLL2-D3RR].
79. See Crowd-Sourced Data, supra note 75.
80. Waze, https://www.waze.com (last visited June 9, 2022).
81. Aaron Pressman &Adam Lashinsky, Why Waze Doesn 't Share Traffic Data with Google Maps-Data Sheet, Fortune (Oct 11, 2019, 5:47 AM), https://fortune.com/2019/10/11/wazegoogle-maps-how-it-works/ [https://perma.cc/2ES9-G6UD].
82. About Waze, Waze Help, https://support.google.com/waze/answer/6071177?hl=en&ref _topic=9022747 [https://perma.cc/YBN7-UXJ4].
83. Another possible source of information would be city awareness apps. For instance, Citizen, a personal safety app, aggregates information from real-time 911 alerts as well as police, fire, and emergency radio transmissions and sends its users location-based safety alerts and related information. See also Using Crowdsourced Data to Estimate Crash Risk, VOLPE Ctr. U.S. Dep'T Transp. (May 14, 2019), https://www.volpe.dot.gov/news/using-crowdsourced-data-estimate-crashrisk [https://perma.cc/K5J5-LYL7]; Dan F.B. Flynn et al., Estimating Traffic Crash Counts Using Crowdsourced Data: Pilot Analysis of 2017 Waze Data and Police Accident Reports in Maryland (2018), https://rosap.ntl.bts.gov/view/dot/37256 (follow "Download Document" hyperlink to access PDF).
84. See Using Crowdsourced Data to Estimate Crash Risk, supra note 83.
85. Sean D. Young et al., Crowdsourced Traffic Data as an Emerging Tool to Monitor Car Crashes, 154 JAMA

Surgery 777, 777-78 (2019).
86. See, e.g., Citizen, https://citizen.com [https://perma.cc/F6WA-4YF3]; see also John Herrmann, All the Crime, All the Time: How Citizen Works, N.Y. TIMES (Mar. 17, 2019), https:// www.nytimes.com/2019/03/17/style/citizen-neighborhood-crime-app.html[https://perma.cc/M9QDF9Z4].
87. Connected Vehicles: CV Pilot Deployment Program, https://www.its.dot.gov/ pilots/cv_pilot_apps.htm [https://perma.cc/4Y3H-SDE9].
88. Qualcomm Tech. Inc., Introduction to Cellular V2X 80-PE732-62 Rev A (2019), https://www.qualcomm.com/content/dam/qcomm-martech/dm-assets/documents/c-v2x_intro.pdf [https://perma.cc/EL75-LEYR].
89. Dedicated Short Range Communications (DSRS), OFF. ASSISTANT Sec'Y for Res. &TECH. U.S. Dep't Transp., https://www.its.dot.gov/communications/media/1probe.htm (last visited June 9, 2022).
90. See Geoffrey Fowler, What Does Your Car Know About You? We Hacked a Chevy to Find Out, Wash. Post (Dec. 17, 2019), https://www.washingtonpost.com/technology/2019/12/17/whatdoes-your-car-know-about-you-we-hacked-chevy-find-out/ [https://perma.cc/EU57-5MZQ].
91. See Connected Vehicle Basics: 20 Questions About Connected Vehicles, OFF. ASSISTANT Sec'y for Res. &Tech. U.S. Dep't Transp., https://www.its.dot.gov/cv_basics/cv_basics_20 qs.htm [https://perma.cc/MZ9C-ZR8D].
92. T-Mobile for Business, Meeting the Growing Demand for Connected Car Data, Forbes (Aug. 28, 2021, 9:00 AM),<https://www.forbes.com/sites/tmobile/2021/08/28/meeting-the-growing -demand-for-connected-car-data/?sh=182c9796b3d8> [https://perma.cc/3VZE-UH89].
93. See, e.g., Meital Ben Sinai et al., Exploiting Social Navigation (Oct. 1, 2014) (unpublished manuscript), https://arxiv.org/abs/1410.0151 (follow "Download PDF" hyperlink to access PDF); Nicholas Tufnell, Students Hack Waze, Send in Army of Traffic Bots, WIRED (Mar. 25, 2014), https:// www.wired.co.uk/article/waze-hacked-fake-traific-jam[https://perma.cc/NS4J-4LA9].
94. See, e.g., Isabella Alexander &Marlena Jankowska, Rights in Geospatial Information: A Shifting Legal Terrain, 41 Melbourne U. L. Rev. 957 (2018); Rebecca Wexler, Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System, 70 STAN. L. Rev. 1343 (2018) Natalie Ram, Innovating Criminal Justice, 112 NW. U. L. Rev. 659 (2017).
95. See Zhenyu Shou &Xuan Di, Similarity Analysis of Frequent Sequential Activity Pattern Mining, 96 Transp. Res. Part C: Emerging Tech.122 (2018); see also GPS Location Privacy, GPS.gov, https://www.gps.gov/policy/privacy [https://perma.cc/D8NZ-CU85] (Dec. 11, 2020).
96. For example, in the United Kingdom, installing and using dashboard cameras is legal and the videos they record can, as a rule, be used as evidence in criminal trials. Felix Wilson, Dash Cams and the Law: What You Need to Know, Which?, https://www.which.co.uk/reviews/dash-cams/ article/dash-cams-and-the-law-what-you-need-to-know-aUty85w5AYQC [https://perma.cc/223PDVMR] (Feb. 17, 2022); In Germany, a dashboard camera may be installed but it may neither record faces nor number plates, due to strict data protection regulations, see Bundesgerichtshof [BGH] [Federal Court of Justice] May 15, 2018, Neue Juristische Wochenschrift [NJW] 2883, 2018 (Ger) (tort case). Whether footage can be used as evidence in criminal proceedings is determined on a case-by-case basis. See 233 NJW 2883 (2886, 2889-90) (Ger.). The same is true for neighboring Switzerland. See Tribunal fédéral [TPF] [Federal Court] Sept. 26, 2019, 6B 1188/2018 (Switz.). While in adjacent Austria, dashboard cameras on windshields are considered illegal. See Verwaltungsgerichtshof [VwGH] [Supreme Administrative Court], Sept. 12, 2016, Ro 2015/ 04/0011, paras. 29 &35 (Austria), https://www.ris.bka.gv.at/Dokumente/Vwgh/JWT 2015040011 _20160912J00/JWT_2015040011_20160912J00.pdf [https://perma.cc/4EDK-T8A9]. For a more general overview, see Darius Štitilis &Marius Laurinaitis, Legal Regulation of the Use of Dashboard Cameras: Aspects of Privacy Protection, 32 COMPUTER L. &SEC. Rev. 316 (2016).
97. See Daniel Lamb, The DashCam Regulations in Each State, GPS Trackit (Aug. 31, 2021), https://gpstrackit.com/blog/what-are-the-dashcam-regulations-in-each-state/ [https://perma.cc/ 3JXF-B557].
98. David Billard &Baptiste Bartolomei, Digital Forensics andPrivacy-by-Design: Example in a Blockchain-Based

Dynamic Navigation System, in PRIVACY TECHNOLOGIES &POLICY: 7TH Annual Privacy Forum, APF 2019, Rome, Italy, June 13-14, 2019, Proceedings 151 (Maurizio Naldi et al. eds., 2019).

99. Blockchain stores data using a growing list of blocks linked in chronological order. Since all users are connected via a distributed peer-to-peer network, they adhere to a protocol and collectively retain control. One of the prominent applications is Bitcoin. See Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System (2008), https://bitcoin.org/bitcoin.pdf [https: //perma.cc/FKV6-P6CJ].

100. Zhuofan Liao et al., Blockchain on Security and Forensics Management in Edge Computing for IoT: A Comprehensive Survey, 19 IEEE TRANSACTIONS ON NETWORK &Serv. Mgmt. 1159, 1168 (2022) (explaining the elements of anonymity, non-tampering, traceability, and transparency).

101. See generally Ming Li et al., Towards Vehicular Digital Forensics from Decentralized Trust: An Accountable, Privacy-Preserving, and Secure Realization, 9 IEEE Internet THINGS J. 7009 (2022).

102. See Mumin Cebe et al., Block4Forensic: An Integrated Lightweight Blockchain Framework for Forensic Applications of Connected Vehicles, 56 IEEE Comm. MAG. 50, 55 (2018).

103. See supra Section II.A.2.

104. See Ziad Amir, Crowdsource Evidence in Digital Evidence Management Software, VIDIZMO: Blog, https://blog.vidizmo.com/crowdsource-digital-evidence-in-digital-evidencemanagement-software [https://perma.cc/Z9LC-M52H] (Mar. 8, 2021).

105. For instance, in 1998, the National Center for Missing and Exploited Children (NCMEC) in the United States began building a database of imagery or videos known to depict the sexual abuse of children. Many technology companies, including Apple, have voluntarily used NCMEC's data to scan their own cloud servers and even customers' phones in search of prohibited material. Cf. A 38-Year-Old Charity Will Be Integrated into Apple 's Newest Operating System, ECONOMIST, https://www.economist.com/united-states/2021/08/14/a-38-year-old-charity-will-be-integrated-intoapples-newest-operating-system [https://perma.cc/V5J3-ZE8M] (Aug. 17, 2021).

106. U.S. Dep't Homeland Sec. Sci. &Tech., Using Social Media for Enhanced Situational Awareness and Decision Support (2014),<https://www.dhs.gov/sites/default/files /publications/Using%20Social%20Media%20for%20Enhanced%20Situational%20Awareness%20> and%20Decision%20Support.pdf [https://perma.cc/A8DS-3762].

107. See Patricia Swann, How the Boston Police Used Twitter During a Time of Terror, PUB. Rel. Soc'y Am. (May 24, 2013), https://apps.prsa.org/Intelligence/Tactics/Articles/view/10197/ 1078/How_the_Boston_Police_Used_Twitter_During_a_Time_o#.YdHBjWjMJaQ [https://perma.cc/ Z2RW-BJFR]; see also Mary Kate Brogan, How Twitter Is Changing Narrative Storytelling: A Case Study of the Boston Marathon Bombings, Elon J. Undergraduate Rsch. Commc'NS, Spring 2015, at 28, https://eloncdn.blob.core.windows.net/eu3/sites/153/2017/06/04BroganEJSpring15.pdf [https://perma.cc/HS2W-59AF].

108. Sophie Bushwick, What the Capitol Riot Data Download Shows about Social Media Vulnerabilities, Sci. Am. (Jan. 27, 2021), https://www.scientificamerican.com/article/what-thecapitol-riot-data-download-shows-about-social-media-vulnerabilities/ [https://perma.cc/64CF-SKEN] (illustrating that seemingly innocuous posts on mainstream platforms can also create vulnerabilities).

109. Katherine Rosman, How the Case of Gabrielle Petito Galvanized the Internet, N.Y. Times, https://www.nytimes.com/2021/09/20/style/gabby-petito-case-tiktok-social-media.html [https: //perma.cc/92QH-X93Q] (Oct. 20, 2021).

110. See Murphy, supra note 33, at 1076; see also Edward Imwinkelried, The Admissibility of Scientific Evidence: Exploring the Significance of the Distinction Between Foundational Validity and Validity as Applied, 70 Syracuse L. Rev. 817, 818-20 (2020).

111. For a vision of courtrooms of the future, see Fredric I. Lederer, Technology-Augmented and Virtual Courts and Courtrooms, in THE Routledge HANDBOOK OF TECHNOLOGY, CRIME AND Justice 518, 525-26 (M.R. McGuire &Thomas J. Holt eds., 2017).

DETAILS

Subject:	Robots; Testimony; Forensic sciences; Automation; Crowdsourcing; Traffic congestion; Vehicles; Autonomous vehicles
Business indexing term:	Subject: Automation
Location:	United States--US
Publication title:	Jurimetrics; Chicago
Volume:	62
Issue:	3
Pages:	285-302
Publication year:	2022
Publication date:	Spring 2022
Publisher:	American Bar Association
Place of publication:	Chicago
Country of publication:	United States, Chicago
Publication subject:	Law, Education
ISSN:	08971277
e-ISSN:	21544344
Source type:	Scholarly Journal
Language of publication:	English
Document type:	Journal Article
ProQuest document ID:	2725644087
Document URL:	http://ezproxy.cul.columbia.edu/login?url=https://www.proquest.com/scholarly-journals/ca-r-veat-emptor-crowdsourcing-data-challenge/docview/2725644087/se-2?accountid=10226
Copyright:	Copyright American Bar Associatio n Spring 2022
Last updated:	2022-10-20

Database:	ProQuest Central

LINKS

Linking Service