The Double Edged Sword that is the Event Data Recorder

The subject is the automotive black box, more accurately described as an event data recorder, or EDR. These devices are analogous to the data recorders used in commercial airplanes (Flight Data Recorders) and on railroad trains (Locomotive Event Recorders). The first 1000 relatively primitive devices were installed in 1974 as part of a National Highway Traffic Safety Administration (NHTSA) project. Their numbers rapidly rose with the introduction and widespread adoption of safety air bags (which became mandatory in 1997) because air bag deployment is controlled by a small computer in each automobile, usually under a passenger seat or within the dashboard, that gathers information about the vehicle's operation to determine when the air bag should deploy. After air bags were first installed, some vehicle occupants claimed that they had been injured by faulty air bag operation. The computer controlling air bag deployment was modified to preserve a record of the data that it monitors. [1] The EDR holds a snip of data that is stored for a brief time, currently about 5 to 20 seconds. This stored information helped evaluate claims about faculty air bag deployment and guided improvements in air bag technology. Alan Adler, the manager of product safety communications at General Motors (GM) says that "The main purpose of the EDR is to get data after a crash to help us understand how the air bags worked." [2] The stored information is also useful for studying the accidents that triggered air bag deployment and various advocates, including the National Transportation Safety Board, the Insurance Institute for Highway Safety, and the American College of Emergency Physicians, have lobbied for the universal installation of EDRs as a matter of public safety.

As currently designed, the EDR deletes the old data as it replaces it with new data, as

---

[1] The Federal Motor Carrier Safety Administration of the U.S. Department of Transportation divides the EDR's functions into four parts: (1) data processing; (2) data storage; (3) data retrieval; and (4) power supply. 14 C.F.R. 135.152 (2004).

[2] Eric C. Evarts, "Is Your Car Spying On You,"Christian Science Monitor, December 27, 2004.

though there were a tape looping back and erasing the displaced entries. However, when an accident occurs, the EDR preserves the prior 5 to 20 seconds of recorded data for possible retrieval, providing a critical snapshot of what happened in the moments before impact. The data that is recorded has expanded from information about deceleration to information that ranges across as many as 16 different parameters, [3] including braking and steering efficiency (i.e., data about brake status, automatic tracking control, and anti-lock braking systems), vehicle speed, engine speed, throttle position, engine fuel management, whether the driver was wearing a seat belt, whether the vehicle's lights and cruise control were on, whether turn signals were used, and changes in velocity (or delta V) in frontal collisions, maximum delta V in near deployment events, and the time between the moment of vehicle impact and the moment of maximum delta V. [4] However, EDRs do not record voices, pinpoint a vehicle's location, or identify who is driving the vehicle. EDRs have been connected to global positioning systems (GPS) installed in the vehicle so that speeds identified by the EDR can be communicated to third parties. [5] This strategy was pursued by a car rental company that sought to impose penalty fees on its customers who exceeded posted speed limits. [6]

EDRs are installed on most newly manufactured vehicles. GM is the industry leader, with Ford following closely behind. Toyota and Honda are also installing EDRs in an increasing percentage of their new vehicles. Mercedes Benz does not install EDRs, though some of the data collected by EDRs are probably accessible in one or the other of the several computer systems on

---

[3] Jeffrey Selingo, "It's the Cars, Not the Tires, That Squeal," New York Times, Circuits, October 25, 2001.

[4] Dennis Donnelly, "Black Box Technology in the Courtroom," Trial, April, 2002.

[5] John S. Ganz, "It's Already Public: Why Federal Officers Should Not Need Warrants to Use GPS Vehicle Tracking Devices," 95 J. Crim. L. & Criminology 1325 (2005).

[6] Christopher Elliott, "Some Rental Cars Are Keeping Tabs on the Drivers," N.Y. Times, Jan. 13, 2004, C6.

Mercedes Benz's new vehicles. [7] EDRs are not required equipment, though, as already indicated, various advocacy groups, including the NHTSA, are campaigning for mandatory installation, at least in new vehicles. The NHTSA has proposed a new rule requiring car markers to standardize black box technology so that data are recorded and stored in the same way and are easier to harvest and compare. [8] The NHTSA estimates that between 65 and 90 percent of 2004 cars and trucks have EDRs. [9]

The information stored in EDRs is useful for the composite data it generates about air bag use and effectiveness and it is also useful in individual instances because it provides information about a vehicle's use and condition in the moments before an accident. [10] This clip of information can prove crucially important. It has already been used in multiple cases to prosecute drivers who were driving at reckless speeds before collisions that caused deaths. However much the drivers insisted that they were driving at reasonable speeds, the evidence that EDRs provided indicating reckless speeds have been admitted into evidence and used to secure felony convictions against the recklessly fast drivers. These are prosecutions in state trial courts and EDRs have consistently satisfied the "general acceptance" standard in Frye hearings. For example, in a January, 2005 case in New York, People v. Slate, [11] the court admitted EDR evidence after an expert, Russell 'Rusty' Haight, Director of the Collision Safe Institute in San Diego, Ca., testified that he had performed 100 crash tests with different cars made by the same manufacturer as the defendant's Corvette and, in a comparison of information provided by EDRs

---

[7] Jason A. Kahl, "Higher Numbers of Black Boxes Used to Spy on Driving Habits of Motorists," Reading Eagle, December 30, 2005.

[8] 49 C.F.R. Part 563, Docket No. NHTSA - 2004 - 18029, RIN 2127 - A172.

[9] Paul Wenske, Car's Black Boxes Stir Privacy Concerns," Charlotte Observer, January 28, 2006.

[10] David M. Katz, "Privacy in the Private Sector: Use of the Automotive Industry's 'Even Data Recorder' and Cable Industry's 'Interactive Television' in Collecting Personal Data," 29 Rutgers Computer & Tech. L.J. 163 (2003).

[11] No. 0666-03, N.Y., Nassau County Sup. Ct.

with objective external instrumentation, he found the EDRs sensing diagnostic modules "extremely reliable." [12] The court explained in its ruling that EDR's underlying technology had been relied upon for years by the government, by vehicle manufacturers, and by crash researchers.[13] The EDRs information is not regarded by the courts as infallible or conclusive. It is subject to attacks on its foundation and on the purpose for which it will be used, i.e., does it have probative value.

The use of EDR data in criminal cases might have run afoul of the Fourth and Fifth Amendments, but thus far neither has much stymied the introduction of EDR data into evidence at criminal trials. [14] Fourth Amendment objections to the reasonableness of police seizures of the EDR are raised in an already inhospitable climate. There are well established precedents that expectations of privacy are considerably diminished when the search relates to an automobile. Automobiles are subject to pervasive, continuing governmental regulation and control, including periodic safety and licensing inspections. They are also subject to police stops for minor infractions or pursuant to an authorized checkpoint. [15] An expression of this disinclination to recognize Fourth Amendment protections for automobile searches is the broad discretion permitted to police officers to search a vehicle after the that vehicle is stopped for a criminal, including a minor traffic, violation. The searches are generally upheld even when their ambit reaches considerably beyond the violation that justified the stop. The 'Carroll Rule' [16] is a generous endorsement of police power to conduct a progressively ambitious search once a

---

[12] Andrew Harris, "Car's Black Box Evidence Ruled Admissible," New York Journal of Law, January 13, 2005.

[13] Sara Hoffman Jurand, "New York Ruling Adds to Growing Support of Black-Box Data," Trial, July 2005.

[14] Kevin J. Powers, "David Hasselhoff No Longer Owns the Only Talking Car: Automobile Black Boxes in Criminal Law," 39 Suffolk University Law Review 289 (2005).

[15] New York v. Class, 475 U.S. 106 (1986).

[16] Carroll v. United States, 267 U.S. 132 (1935).

legitimate stop has occurred.

Inventory searches represent a further reduction of Fourth Amendment protections in automobile cases. Such "inventories pursuant to standard police procedures are reasonable" [17] even without probable cause to believe that the vehicle contains evidence of a crime because, as we know so well, automobiles involve a diminished expectation of privacy. It is noteworthy that exigent circumstances are not required to support an inventory search. Inventory searches tend to be regarded as, by their very nature, reasonable. In the context of an accident, especially a fatal accident, inventory searches are presumed to promote public welfare rather than transgress protected liberties. In leading state EDR case the court ruled that there is "only a diminished expectation of privacy in the mechanical areas of the vehicle [which] must yield to the overwhelming state interest in investigating fatal accidents." [18]

Fifth Amendment objections that EDR data is a form of self-incrimination have similarly proved ineffectual. It isn't clear that EDR data will be regarded as testimonial rather than as real or physical evidence. Even if it is regarded as testimonial evidence, police access to support accident investigations will likely be regarded as an essentially "regulatory" action. Following U.S. v. Byers, which upheld a state regulation that required drivers to disclose their names to an investigating police officer when the driver was involved in an accident, courts are likely to view EDR data retrieval from accident scenes as a lesser and unobjectionable intrusion. The seizures will be justified by the general purpose of promoting public welfare, rather than their impact upon a "highly selective group" suspected of criminal conduct: "[D]isclosures with respect to automobile accidents simply do not entail . . . substantial risk of self-incrimination." [19]

Insurance companies have introduced information from EDRs in civil suits to rebut

---

[17] South Dakota v. Opperman, 428 U.S. 364 (1976).

[18] People v Christmann, 776 N.Y.S. 2d 437, (N.Y.J. Ct. 2004).

[19] California v Byers, 402 U.S. 424 (1971).

claims that air bag malfunction or other vehicle defects caused damages to the driver or passenger plaintiff. [20] Although there are critical issues about who should have access to EDRs under what circumstances and lesser, though still relevant, questions about whether the EDRs are tamper proof and/or appropriately resistant to accidental spoilation, [21] the basic technology permits ready and repeated access to the EDR and its stored information. In 2000, Vetronix released a Crash Data Retrieval System that permits a user to connect a notebook computer to an EDR, download the recorded information, and display the data as graphs and tables. [22] Most car makers encrypt the data, making it inaccessible to the public, including the vehicle owner, unless they can afford Vetronix's System or otherwise have access to that system. [23] However, there are after market, piggy back systems that do permit access to their accumulated data. [24] The storage capacity can be modified fairly easily to accommodate hours or days of data rather than 5 to 20 seconds. Some parents have modified their EDRs with a CarChip, a black box that records up to 300 hours of driving, to monitor their children's driving practices.[25] The information from the CarChip can be downloaded onto a home computer, providing a detailed report on the vehicle's operation. The EDR can also be modified (one such device growls) to alert the driver when safety thresholds for braking or turning are exceeded. Progressive Insurance is running a pilot program in Minnesota which provides discounts to participants who make their EDR records

---

[20] For example, in Backman v. General Motors Corp., 332 Ill. App. 3d 760 (200), GM introduced data to show that the plaintiff's air bag did not malfunction. The jury returned a verdict for the defense.

[21] David Uris, "Big Brother and A Little Black Box: The Effects of Scientific Evidence on Privacy Rights," 42 Santa Clara L Rev. 995 (2002).

[22] Richard J. Newman, "No Place to Hide," U.S. News and World Report, July 14, 2003.

[23] The cost of the system was $2,500.00 in 2004. Christian Harlen Moen, "California Protects "Black Box" Auto-Crash Data from Disclosure, Trial, Dec. 2003.

[24] Robert David & Jayne O'Donnell, "Black Boxes for Cars Slow to Catch On," USA Today, Money, June 3, 2005.

[25] Michelle Higgins, "A Back-Seat Driver for Your Teen's Car," Wall St. J., Feb 23, 2005.

available to the insurer and thereby are able to demonstrate safe driving practices. [26]

These practices contrast with warnings about the complexities of reading reports generated by an EDR, at least when using the information to explain how an accident occurred. Some have expressed concerns that the information will be not be interpreted competently. "The data can be misleading if you're not a seasoned accident reconstructionist," claims Bob Kreeb, a Booz Allen Hamilton engineer who chaired a committee of the Society of Automotive Engineers to establish standards for the data generated by EDRs. "The information needs to be interpreted and validated." [27] A related concern about EDRs is that they detect movement when its principal direction and the principal direction of force is forward. Movement relating to rear end and side impact crashes are often not detected by the EDR. [28] When a vehicle is rotating, spinning, or skidding sideways, significant information about the vehicles speed and movements cannot be measured by the sensors in the EDR and therefore are not recorded there. [29]

If the meaning of the EDR data presented at trial isn't clear without an expert's assistance, the quandary is whether we should depend upon expert interpretations, or insist that the mechanism's operation be apparent to the lay juror, or aim for some intermediate point where the jury grasps the foundations of the science, if not its finer subtleties. Thus far courts generally have been persuaded that the underlying science is sound and that its results are probative and that therefore EDR evidence is admissible. An Illinois court dismissed concerns about the uniformity of the several EDR systems because the underlying technology shared by all EDR systems was well established, "subject to peer review" and not "a novel technique or method." [30]

---

[26] Evarts, supra, note 2.

[27] Id.

[28] Mark Joye, "Big Brother or Big Savior? Here Comes the Black Box," 16 South Carolina Lawyer 38 (2004).

[29] Donnelly, supra, note 4.

[30] Bachman, supra, note 20.

This information about a vehicle's operation is relevant to an insurance company that is assessing the risks of insuring a driver, or, more particularly, determining whether an accident claim by one of its insured should affect that insured's premium. The prospect of insurance company pursuit of EDR records has prompted many states, 17 at last count, to bar insurance companies from using EDR information to set automobile insurance rates. The legislation usually permits the information to be retrieved without the owner's consent for medical research or motor vehicle safety purposes, though without disclosure of the driver's identity, or pursuant to a court order, which would entail disclosure of the driver's identity. [31] Otherwise, the legislation reaffirms that the EDR is the property of the vehicle owner and prohibits an insurance company from conditioning its coverage or the payment of a claim on permission to access the EDR. GM has adopted the policy that it will not access EDR data or share it without the consent of the vehicle's owner unless there is a court order.[32] The difference between requiring access to EDRs as a condition of coverage and encouraging the grant of permission to access EDRs with discounted premiums will have to be sorted out. It is worth noting that when a vehicle is totaled, the insurance company usually insists that the insured sign over title as a condition of paying the property damage claim, after which transfer the EDR belongs to the insurance company. Note further that there is no federal statute law governing who has access to the information from EDRs or how it can be used. [33]

Privacy advocates generally concede the usefulness of EDR information for accident reconstruction purposes. Information gathered from EDRs is more useful than crash test results because it includes real world crash impulses, i.e., the energy generated by the rapid deceleration on the vehicle and its occupants, and because it can be correlated with real world injuries and fatalities. Instead of BOGSAT (bunch of guys sitting around talking), there is real data. The

---

[31] John G. Spooner, "Rocky Road for Car 'Black Boxes,'"CNET News, March 9, 2005.

[32] Wenske, supra, note 9.

[33] Eric Kelderman, "Lawmakers Restrict Use of Crash Data from Recording Device," Arizona Capital Times, October 7, 2005.

information makes accident reconstruction more objective and provides a factual basis for regulatory and consumer information initiatives. With fatal accidents, the vehicles are part of a crime scene investigation and can be secured in place until warrants for access to EDRs are obtained. With non-fatal accidents, investigators can act to obtain warrants before vehicles are moved if they adduce evidence satisfying the governing standard that a crime has been committed.

However, privacy advocates are concerned that most vehicle owners and operators have no idea what EDR technology is or what information it is gathering. [34] Not knowing these fundamental facts about EDR, they do not know the rules that govern who can access the EDR and on what grounds that access is justified. The fear is that a devise designed to protect the automobile manufacturer from defective product liability and thereafter enlisted in a public safety campaign to generate a reliable database about accidents will be used without safeguards to gather evidence for law enforcement and insurance defense purposes. As David Sobel of the Electronic Privacy Information Center has stated, "The legal structure that is going to control how this information is going to be used hasn't been developed yet. We need some legal protection in place to make sure that only five seconds of driving information is collected, rather than five minutes worth or five hours. With storage media becoming so inexpensive, there's going to be a tendency to collect more and more of this information."[35] There is a corresponding interest among parties other than the driver / owner to gain access to that information.

Two potential future developments concern privacy advocates. As we have seen, EDRs can be modified fairly easily to record more than a 5 to 20 second clip of information. Mission creep, e.g., relating to the generation of composite data about accidents, may gradually extend the length of the clip to several minutes. The reformulation of EDR's mission to explicitly support the investigation of particular accidents could lead to even lengthier records of vehicle use. Fleet

---

[34] Dorothy J. Glancy, Privacy on the Open Road," 30 Ohio N.U. L. Rev. 295 (2004).

[35] Paula Zahn Show, "Car's Black Box May Invade Privacy," CNN, August 20, 2004.

vehicles provided to employees or independent contractors are a likely occasion for the use of EDRs with extended memory chips. Trucking companies have already adopted the technology to track the operation of their vehicles. Although the trucking industry has not yet taken a uniform position on EDR technology, many individual truck owners are convinced that monitoring their trucks promotes both their pecuniary interests and public safety. [36]

The increased use of GPS systems in vehicles and their connection to EDRs is the second problematic development. GPS technology is being adapted for increasingly many products, e.g., in cellphones, because it can identify a user's location in cases where the user cannot, e.g., because they are lost or disoriented. GM has been developing an optional Advanced Automatic Crash Notification (AACN) system as part of its OnStar GPS system. The sensory diagnostic module of the EDR would report information about an accident to an OnStar adviser who would relay that information to emergency medical personnel to assist with the identification of appropriate equipment and services to deliver to the accident site. [37] However, with a GPS connection the driver would face difficulties controlling access to the information acquired by the EDR. That information would be available to whomever had access to the EDR - GPS system installed in the vehicle. It may prove difficult to limit access to that system to only those denominated by the vehicle owner. Whatever access limitations might be sought, a public safety exception would likely be carved out to address special situations where a life is endangered or otherwise the benefits of accessing the EDR - GPS system seem overwhelming. The exceptions would likely expand over time. They might expand to accommodate much more mundane public safety issues, like speeding on public roadways.

Both prospects involve a monitoring of the driver's use of a vehicle. The devices are generally regarded as the property of the vehicle owner, therefore within the owner's control, so

---

[36] Donald C. Massey, "Proposed On-Board Recorders for Motor Carriers: Fostering Safer Highways or Unfairly Tilting the Litigation Playing Field," 24 S. Ill. U.L.J. 453 (2000).

[37] Rachel Konrad, "Car-tracking System Raises Hopes, Concerns," CNET New, August 1, 2002.

that they can be disabled at the instigation of the owner. They might instead be regarded as safety equipment for which disablement is prosecuted and penalized, e.g., as in the case of a catalytic converter. Even if the EDR or the GPS linked EDR legally can be disabled, it is likely that most owners will not modify their vehicles. Instead, the inconvenience and / or the cost of disabling the system, or the concern that disabling the EDR will disable the air bag safety system, which it does, will lead to a less private world in which driving practices are subject to the steady scrutiny of unnamed third parties. We may not need radar guns, whether operated by police officers or linked to automatic photography technology, to enforce traffic laws. We may let the vehicles enforce these laws for us. [38]

EDR technology confers benefits and poses challenges. As with other evolving surveillance technologies, e.g., GPS in cell phones and radio frequency identification chips in consumer merchandise, the ostensible primary purpose is limited in scope, often phrased in terms of consumer protection. EDR technology builds upon the requirement of a dedicated computer within each vehicle that controls air bag deployment. With this foundation in place, small modifications permit the recording of the monitored data and the retrieval of that record. The initial motivation for the generation of a retrievable record was to defend against claims that the air bag system had malfunctioned and caused personal injuries and to enable improvements to the deployment system. Those motivations seem entirely reasonable. Why shouldn't a manufacturer take steps to defend itself against liability, especially when those steps could both deflect liability in many instances and provide useful information with which to improve the technology and the protection that it provides (coincidentally further reducing future liability claims). Given that the data had been compiled for these purposes, it was a downhill stretch to en-analyze the data in broader terms to promote a better understanding of vehicle and operator behavior before accidents. The data in the EDR was relevant to a host of questions about these behaviors and the quantity of available data enabled scientific studies that compiled, compared

---

[38] April A. Otterberg, "GPS Tracking Technology: The Case for Revisiting Knotts and Shifting the Supreme Court's Theory of the Public Space Under the Fourth Amendment," 46 B.C.L. Rev. 661 (2005).

and contrasted quantified data. Access to EDR data for automobile accident analysis promised a bounty of invaluable information and, not surprisingly, a coalition of concerned parties argued persuasively to make the data available. [39]

One of the component features of a market economic orientation is an openness to reformulating knowledge of one sort into another sort that is potentially profitable. A market culture encourages this kind of creativity; innovators and the users of their products often flourish when something intended for one purpose is adapted to other purposes. It is hardly surprising that access to composite data from multiple accidents in order to assess causal relationships would inspire a narrower focus on individual instances to evaluate the behavior of particular vehicle operators. It is likely that this individualized focus was countenanced from the beginning, but the rationale for this use, despite the lack of notice to the vehicle owners about the presence of the EDR or its contents, piggybacked on safety justified access to composite data. However it developed, both criminal prosecutors and insurance companies have strong interests in the data compiled by EDRs and have already accessed that data in multiple cases. The trend is likely to persist and, though threshold conditions will be identified, those thresholds will be crossed on a routine basis. Successful use of EDR data will breed expanded uses. EDR access will likely become standard procedure for accident investigations in both criminal and civil areas. Already trial practitioners are being counseled to include requests for EDR data among their routine automobile accident procedures.

The data retrieved from EDRs is clearly relevant to the investigation of accidents. Why balk at a trend to routine access to the EDR? The answer isn't easy to articulate because it is formed in the shadow of the suspicion that resistance seeks to protect wrongdoing, i.e., there is no reason to fear access to EDR data if the vehicle operator was obeying the relevant traffic laws. This is a recurring theme in surveillance related debates: it is only criminals who need fear third party observation of their behavior. Yet this is a distortion of the issues at stake. It isn't only

---

[39] Thomas M. Kowalick, FATAL EXIT: THE AUTOMOBILE BLACK BOX DEBATE, Wiley-EEES Press (2004).

criminals who resent undesired observation of their behavior. A stalker need do no more than follow and watch to unnerve the focus of the stalking. Even if the victim recognizes that there is no threat of physical harm, the stalking remains objectionable. The victim does not want to be and should not be made the subject of unwanted attention. The individualized attention of the stalker is different than the global reach of most surveillance technology, but there are similarities. We behave differently when we know that we are being observed and, though we may occasionally seek out such situations, e.g., as actors, or public speakers, or teachers, we want to determine when we are being observed.

The crux of the explanation for this desire to live away from the gaze of others is personhood, i.e., the life project of defining one's person and character. This defining is a process, an ongoing activity with evolving standards and models. The self is usefully envisioned as an organizational principle, a means of coordinating our experiences as a unified narrative that undergoes continual revision under existentially uncertain conditions. Our calculus for self-evaluation is organic and dynamic; the tasks that force us to refine and reformulate our self-definitions arise in an infinite variety of forms. "The self is an attitude that can change dramatically under appropriate conditions toward integration or disintegration." [40] We cannot rely upon our own postulations about who we are because we are social beings. We rely upon others for nourishment and guidance when young and we are inextricably linked to the mores and beliefs of those with whom we learn how to survive. Yet we do not want to let the task of shaping our sense of self be taken up by just anyone because we have reason to be cautious of the motives and understandings of most of those who know us only fleetingly, with little appreciation for our unique histories. We instead hold out for a layered approach in which intimates of various degrees are relied upon to reinforce our preferred judgments about who we are. The exact phenomenology of this project need not be specified in exact terms for its impact on surveillance technologies to be apparent. If it is true that we are reluctant to expose ourselves to the unsympathetic, dismissive judgments of others in lieu of a more nuanced and narratively

---

[40] Ariel Glucklich, SACRED PAIN: HURTING THE BODY FOR THE SAKE OF THE SOUL, (Oxford, 2001)

rich account available from our relatives and friends, then we will resent and resist the imposition of the former upon us.

As I have phrased this project of defining oneself, it may seem that efforts to shield against unwanted and unsolicited judgments are unacceptably vain and fearful. One's account of oneself should stand the light of public display and the criticism of others. Honest appraisals and forthright expressions of them are important to the construction of a realistic and consistent self. However, those critical assessments are more likely constructive when they are informed by the particular history of the subject. Indeed, it is difficult to evaluate a point in time without knowing the trajectory of its movement; a richer account of its past locations and the influences previously exerted upon it provides a more complete and meaningful evaluation. We rightly suspect that our intimates are more likely to appreciate the context of our lives as they counsel us about what we have done or plan to do next. There is surely a need for evaluators who know nothing about the person other than the performance, but we are loathe to reduce ourselves to a series of performances disconnected to the complicated narrative of our lives. We rightly limit the number of occasions when we are evaluated a-contextually, especially if that evaluation is not keyed to a discrete skill, but instead portends a grander sweep, perhaps with imperious and summary overtones.

The focus upon context helps explain why we regard snapshot judgments about us as objectionable. We might generally be graceful, but fear that one awkward slip will affect judgments about our physical dexterity. Those who know us recognize the slip for an exceptional incongruity. Those who do not may judge us by the exception rather than by the rule. Of course, this problem of misunderstood exceptions is hardly new, but it presses harder when modern technology permits a permanent record of the exception. One miserable moment may linger long in infamy when there is a permanent record of its appearance, however brief and out of character that moment may be. Surveillance technology underwrites the prospect of capturing those out of character moments and subjecting us to harsher criticisms than a momentary lapse would otherwise justify.

There is a recent example of how this fear of revelation can diminish personhood, though the example doesn't rely upon sophisticated technology so much as the ubiquity of observation that expanding surveillance technology promises. The example is the practices of the police in the formerly Communist states in Eastern and Central Europe. The police relied upon vast networks of informers supplemented by a bureaucracy that hoarded written records about every citizen. The result of this comprehensive surveillance was a vaguely paranoid - schizophrenic citizenry. Most people were extremely cautious about what they said publicly because they supposed, correctly, that informers would report on what they said. Honest conversation was restricted to a severely constricted group of trusted colleagues and family. Even within these groups, there were often doubts about the reliability of particular members, either because they were police plants or because their priorities might change when they could gain something by turning on their former confidants.

This pervasive fear of exposure had curious impacts. For example, many professors read assigned texts verbatim to their students for the duration of every class period. Partly this can be explained by the difficulty of acquiring textbooks, but it was also a means of anticipating and deflecting criticism that something objectionable was stated in a classroom. If someone else approved the textbook and all that the professor did was read the approved text, then there was no chance that anything objectionable would be uttered during a class. Students, too, avoided unsanctioned expression. The papers that they wrote for classes were often cribbed directly from texts. The students rearranged the order of the sentences, but not their contents. Not surprisingly, these papers were not graded down for plagiarism. Rather, the student indicated an awareness of how to avoid the generation of potentially incriminating statements. Of course, neither the professors nor the students were criminals who were trying to evade detection. Rather, they were normal citizens who recognized that if some untoward event occurred later in their lives the record of their prior life would be re-examined in excruciatingly fine detail to identify evidence of a longstanding unreliability. The prospect of prosecution for unstated crimes, a la Franz Kafka, was a permanent concern and many people devised strategies to minimize the possibility of ambiguity in their official records.

Surveillance technologies can function in the same manner. You may claim to be a safe driver, but a constant surveillance of your driving practices might reveal a steady stream of violations. Many of the violations would be identified out of context so that rolling through a stop sign at 3:00 a.m. on an empty street is categorized with running a stop sign during rush hour. Speeding on a open road may look the same to a computer as speeding on a very busy roadway. Of course, in either case the law has been broken. But the failure of context undermines distinctions between technical violations that do not evidence dangerous propensities and egregious violations that do. Indeed, a computer might detect multiple violations for a driver who regularly drives on isolated roads and identify that driver as an insurance risk or an otherwise especially dangerous driver. It might generate no reports for a driver who often changed lanes dangerously because that behavior is undetected by the device. The point is not to excuse any violation, but to highlight the failure of context with which to evaluate the severity of the violation. An EDR with a long memory could generate data that indicated violations without providing sufficient context for those violations to support informed judgments about how the information should be used.

The challenge of the EDR is manageable and current efforts to condition access to its data indicate an appropriate resolve to harness the technology. Those efforts may seem overzealous to some who have not thought carefully about the potential effects of future, unrestrained use of the technology. As is often the case with surveillance technologies, its benefits can blind us to the darker implications of misuse. With surveillance technologies the danger is especially pronounced because the benefits are often immediately appreciable and those benefits are loudly touted by the industry that profits by their proliferation. The costs arise as a function of slowly accumulating pressures as surveillance expands to its vast technological compass.