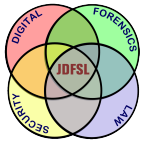

THE JOURNAL OF DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 10 | Number 4 Article 4

2015

Cyber Black Box/Event Data Recorder: Legal and Ethical Perspectives and Challenges with Digital Forensics

Michael Losavio
University of Louisville

Pavel Pastukov
Perm State National Research University

Svetlana Polyakova
Perm State National Research University

Recommended Citation

Losavio, Michael; Pastukov, Pavel; and Polyakova, Svetlana (2015) "Cyber Black Box/Event Data Recorder: Legal and Ethical Perspectives and Challenges with Digital Forensics," *Journal of Digital Forensics, Security and Law*: Vol. 10 : No. 4 , Article 4.
DOI: https://doi.org/10.15394/jdfsl.2015.1210
Available at: https://commons.erau.edu/jdfsl/vol10/iss4/4

CYBER BLACK BOX/EVENT DATA RECORDER: LEGAL AND ETHICAL PERSPECTIVES AND CHALLENGES WITH DIGITAL FORENSICS

Michael Losavio
University of Louisville
Department of Criminal Justice
Louisville, Kentucky 40292 U.S.A.
michael.losavio@louisville.edu

Pavel Pastukov
Perm State National Research University
Department of Criminal Procedure and Criminalistics
Perm, Russian Federation
pps64@mail.ru

Svetlana Polyakova
Perm State National Research University
Department of English Language and Intercultural Communication
Perm, Russian Federation
polsvetlana@yandex.ru

ABSTRACT

With ubiquitous computing and the growth of the Internet of Things, there is vast expansion in the deployment and use of event data recording systems in a variety of environments. From the ships' logs of antiquity through the evolution of personal devices for recording personal and environmental activities, these devices offer rich forensic and evidentiary opportunities that smash against rights of privacy and personality. The technical configurations of these devices provide for greater scope of sensing, interconnection options for local, near, and cloud storage of data, and the possibility of powerful analytics. This creates the unique situation of near-total data profiles on the lives of others. We examine legal and ethical issues of such in the American and transnational environment.

Keywords: event, data, recorder, legal, ethical, privacy

1. INTRODUCTION

Digital forensics is the search for reliable evidence within electronic information. One problem that has been characterized as the "terabyte problem" is that the size of a data corpus may grow beyond that which can be properly analyzed forensically. But the inverse of this is that within these massive data collections we have far more information on the lives of others than in the past and subject to examination in ways never before previously possible.

This implicates serious issues of the nature of personal privacy and autonomy within the processes of digital forensics. These issues, in turn, may challenge the foundational legal

principles of states protecting those interests, foremost among them for the American polity being the Fourth Amendment to the United States Constitution and the right it guarantees its citizens that they will be secure in their persons, houses, papers and effects against unreasonable searches and seizures by the state.

The information of the lives of people is generated in and through many roles. These can be considered as nodes tied to the different domains of basic life activities and functions:

Personal Life

Work Life

Home Life

Transport

Social Life

(Elmaghraby & Losavio, 2014).

Each of these may overlap with others. Each may generate precise data from which a detailed and granular life profile is painted. This data may connect an individual with location, transactions, activity, time and proximity. The legal implications of this should be anticipated and addressed.

The growth in "Event Data Recorders" (EDR) in all forms and sizes produces special challenges for the forensic collection of this information. The political debates regarding the technical factors of encryption and data protection in such devices are built on fundamental questions of law and ethics that should be considered as part of the analysis of any technical implementations.

From ancient times people have sought to memorialize their travels, whether with the ancient Greek periplus or English sea captain's rutter. These served as accounts of travels and guides for the future, like the personal journals kept by travelers. These media required the survival of the medium and, usually, the author to make their way to others and inform the general world. With the ship lost at sea, so often would the journals of crew and passengers pass into the deep, with nothing to tell of their passing.

The evolution of transportation systems was matched by the evolution of methods to record transportation activities. The increasing capital costs for transportation systems and the commensurately greater damage they could do upon failure may have been an impetus for this. Train event recorders were introduced in the late 19th century to record time and speed data on locomotives (HaslerRail, 2015).

With the deployment of the first jet airliners came efforts to record and preserve information that might explain the cause or causes of catastrophic airplane crashes. Australian David Warren developed his "Flight Memory Unit" as a way to record the voice of the pilots and flight instrument data to help determine the cause of a crash (Paur, 2010). The first versions of the device were produced in 1957, to objections that their use would constitute an invasion of privacy. Australia was the first country to require the use of these devices in crash and fireproof containers.

The experience of the aviation industry with the black box showed its utility in both resolving the causes of aviation incidents and directing efforts to enhance safety and reliability in aviation transport. It is a model that has expanded into other areas of transportation.

With the development of cost-effective technologies for event data recording, the use of these devices expanded into other transportation technologies. Commercial transport companies began to use EDR devices to monitor work performance and as evidence in accident reconstruction cases. Beginning in the mid-1990s similar instrumentation was mandated in the United States for all new car

sold in the domestic market. These matched use of On-Board Diagnostic computers (OBD) for monitoring and evaluating engine condition and operations.

More extensive data recording was implemented in automobiles through EDR devices that were also called "black boxes." The EDR devices began to collect additional information regarding vehicle activity and performance which would then be preserved for later analysis.

The US regulatory agency for vehicle traffic systems, the National Highway Traffic Safety Administration (NHTSA), set out through regulation the required types of data the systems must collect, the format and the durability and survivability of the recordation medium (49 CFR Part 563, 2015). Vehicle systems and data opportunities are also created by the global positioning satellite systems and communications systems, such as cellular phones, used in vehicles. These devices may provide information directly to EDR recorders or may independently preserve that information in their own systems.

Video of vehicle and external activity can also be captured and stored, revealing events that occurred at key times within the vehicle. Apps are now available to use a cellular Android phone to collect vehicle event data and video (AutoGuard Dash Cam, 2015).

This is a data space for transportation systems that while once autonomous are now subject to the collection of significant amounts of data at a consumer level rather than only at the level of mass transportation.

Paralleling this is the rise of hyper-personal instrumentation through smart phones and peripheral devices that can log in record massive amounts of information about the lives of individuals. This data can range from key GPS locational data to health and physical activity information to journal information from the device user in text, audio and video forms.

Given the interconnected nature of such systems, this, too, creates a huge data corpus that may be both resident locally on an individual system as well as in storage in the cloud.

The advantage of a highly interconnected set of event data recording systems is preservation through real-time backup of key data maintained in the cloud rather than just locally. This debate is a result, in part, of the Air France and Malaysian air disasters for which forensically useful event data could not be retrieved or was never found.

This highlights the twin challenges of forensic accessibility in these highly mobile devices and the intense privacy concerns which may now accompany the profiles of people in ways never before possible. We explore these issues.

2. PERSONAL AND AUTOMOTIVE EDR SYSTEMS

Americans have a deep affection for two particular pieces of their technology, their cellular telephones and their automobiles. Given the central role these play in their lives and the immense data about those lives the systems can generate, they've come to play key roles in legal and judicial resolution of issues in people's lives, whether from accidents, infidelity or crime. Given the questions raised as to privacy and who really "owns" the data about someone's life, naturally leads to legal and policy challenges. Details of these legal and policy concerns are detailed below.

2.1 Automotive Data Systems

As automotive data systems pull data from sensors within the vehicle, they collect panoply of information that can, in turn, offer guidance

as to what a driver has been doing and what the driver may have done prior to an incident. For the OBD/EDR (Event Data Recorders) data that may be collected include vehicle status, airbag deployment speed, seatbelt usage, acceleration, and braking. In one case the lieutenant governor of Massachusetts was fined after an accident where the "black box" recording showed he was driving 100 mph; this also led to a police retraction of an earlier report that the cause of the accident was due to ice on the road (Bierman, 2012).

The growth in hands-free messaging and telephony, GPS navigation systems and onboard Internet access provide even vaster onboard information regarding the activities of the vehicle and of the driver. The hands-free telephone and messaging collects and tracks telephone and contact numbers called, messages and texts, often with metadata showing the times such communications were made and whether incoming or outgoing. The GPS navigation systems store trip data, home site and backtrack data of route taken. These provide forensic opportunities where such data analysis is necessary.

Forensic use of this data, from investigation to litigation has been growing, such as in investigation and the prosecution and defense of vehicular homicide cases where it has been called "an unbiased witness to the truth". (Sharp, 2003) Vehicle manufacturers themselves have used the data in civil litigation where they are the defendants to show that, in fact, user error was the cause of an accident rather than a vehicle failure (*Batiste v. General Motors Corporation*, 2001). Data correlation of cell phone text use in vehicular homicide cases involving teenagers led to a nationwide movement to legally prohibit and socially disapprove of texting while driving in the United States.

2.2 Personal Data Systems

This scales up in terms of the scope and diversity of data collected with personal cellular phones: indeed, 64% of U.S. residents own "smartphones" with advanced capabilities" (Smith, 2015) "Smart phones" and their sensors can collected data on physical movement, location, transportation, sound, images and physiological parameters; enhanced features can collect a wider variety of actions and conditions, including personal health information. (Cnossen, 2015) Health futurists see opportunities to link this mobile data with genetic, medical and environmental (physical, social, behavioral) data for both research and personal health improvement.

Cellular telephones store the data lives of their holders in ways never imagined. In turn, they have become the darlings of the evidentiary and forensic communities, whether for criminal investigation or preparation for divorce court. Some have characterized the user's smart phone as "the single most valuable new police tool." (Kaste, 2014). One study of a newly introduced digital forensics capacity to a small city police force found that the examination of cellular telephones quickly outstripped the need for forensic examination of computing devices. This department's data indicated, *inter alia*, the expanding useful of cell phones a as evidence sources in more and more traditional areas of law enforcement, as seen in Table 1 (Losavio, Keeling, Lemon, 2012).

Table 1
Comparison of Numbers of Devices Examined (2012 SADFE/UNESCO Conference)

Sept. 2011 - July 2012	**# Computers**	**# Cell phones (SIMs included)**	**Other**
September		6	
October	5	18	1
November		5	
December		7	
January		2	1
February	3	13	7
March	2	10	3
April		9	4
May	1	4	3
June	2	9	2
July	1	5	2
totals	**14**	**88**	**22**

3. EVOLUTION OF AMERICAN LEGAL STANDARDS FOR THE ACQUISITION OF EVENT DATA

Although there is a growing body of case law regarding conduct with automobile event data recorders, the pervasiveness of cell phones has put them in the lead for creating the legal conflicts that generate case law under American law.

Part of the legal and ethical conflicts relate to privacy (Mueller, 2006). This data can reveal a great deal about a person's activities. One United States Supreme Court justice, in commenting on the nature of GPS monitoring in the case of *United States v. Jones* observed that such tracking could reveal family, professional, and many other types of associations all based around locational data (*United States v. Jones*, 2012).

The legal issues relating to cyber black box data collection fit within the framework of privacy rights as established under the Fourth Amendment to the United States Constitution. The Fourth Amendment prohibits a state seizure or search absent probable cause that evidence of a crime is present and that a judicial warrant for that search or seizure is issued by a neutral magistrate. There are a variety of exceptions to this based on balancing issues of public safety against the privacy rights of the individual. A warrantless search is reasonable only if it falls within a

specific exception to the Fourth Amendment's warrant requirement.

But several justices in the *Jones* case observed that GPS tracking with electronic aggregation and analysis created a radically different technology and scale of data profiling that presented special issues needing resolution.

These issues of technology and scale are clearly presented by the nature of data collection for the cyber Black box. The foundational cases in the United States that begin this analysis are the 2014 Supreme Court opinions of *United States v. Wurie* and *Riley v. California.* The Supreme Court discussed the massive amounts of information which electronic devices can store such that there would be a reasonable expectation of privacy in such devices that should not be violated where they are seized as part of an arrest of a suspect. This doctrine allowed officers of the state to circumvent the Fourth Amendment protective requirement of a warrant to search issued by a neutral magistrate based upon a finding of probable cause that evidence of a crime would be found. It allowed for a great deal of police intrusion into private affairs were there were no other legal grounds pursuant to the Fourth Amendment.

At issue in these cases was the data stored in that most popular of portable personal data devices, the cell phone. Under prior case law, a person placed under arrest could be searched and the things found on them searched under the doctrine known as "search incident to an arrest."

But the challenge presented in diverse cases across the country was whether or not this doctrine could withstand the changes in technology where so much, if not most of a person's life might be found in that personal device.

The legal principles and policy concerns at issue in a search incident to an arrest doctrine were 1) need to protect a police officer from an arrestee, 2) the need to protect potential evidence that might be destroyed by an arrestee and 3) the counterbalancing privacy interest of the person being arrested. The Supreme Court observed that deviations from the warrant requirement might be justified only by first "...assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.," citing *Wyoming v. Houghton*, 526 U. S. 295, 300.

In conducting its analysis the Supreme Court found that the cell phone device did not create a risk or danger to a police officer during the arrest. Further, it found that there was no danger of the destruction of evidence once the device was secured from the arrestee. This then was weighed against the massive amounts of information now stored in these devices. Given this technical change in privacy interests weighing heavily in favor of the individual, the Supreme Court held that the search of the device could only be done once a warrant had been secured after finding of probable cause that it contained evidence of a crime is determined by neutral magistrate.

Given the nature of this data and the personal information it may reflect, this will have an impact regarding the necessity of search warrants for the seizure of such information or some kind of court process regarding its access. This invokes the panoply of Fourth Amendment requirements to justify a state seizure of this information.

This application of these basic legal principles can be applied to other areas as to the seizure of information.

3.1 The "Automobile Exception," Cell Phones and Auto Event Data Recorders

The special legal principles at issue in the "automobile exception" to the requirement of a warrant in order to seize and search at automobile are built around the concepts that 1) the automobile is mobile and may easily move beyond investigative jurisdiction, 2) it is out in the public and thus subject to a lesser expectation of privacy and 3) it is subject to government regulation which, again, reduces the level of expectation of privacy.

This has implications for automobile event data recorders, particularly where they have been involved in activities such as an automobile collision or traffic violation where probable cause exists to believe the EDR contains evidence relating to a crime. This may apply equally to cell phones to the extent that they are highly mobile with some aspects of action in public. The split with traditional search and seizure doctrine is that implied by *Wurie* and *Riley* is that while these devices may be seized, they may not be searched without first applying for a warrant. While this may seem to be only a technical issue, a neutral magistrate's evaluation of the sufficiency of the basis for probable cause may differ from that of investigating police officer.

These facts raise issues as to the right of a police officer to search an event data recorder after a collision or traffic violation. The officer may have a right to seize or otherwise preserve the data in the EDR if there is a reasonable threat that the information may be destroyed or lost; that officer would then have an obligation to timely seek search warrant to examine it for information. If the vehicle has been legally abandoned or turned over to the custody of others, then there may not be Fourth Amendment implications for the examination of the data if that device is no longer legally in the possession of the automobile's owner. The seizure of the vehicle by police may raise additional issues, as discussed in the section on inventory searches, below.

Increasingly other privacy-protecting legal restrictions may apply that limit access to the information, such as statutory limitations or requirements for consent or a court order even where the vehicle is no longer physically under the control of the owner (California Vehicle Code § 9951(c)(2), 2015) (*People v. Xinos,* 2011).

3.2 Exigent Circumstances

The exigent circumstances exception essentially permits seizures and searches under and objectively reasonable determination that emergency circumstances justify the action, even if the emergency circumstances or the result of a police officer's unlawful actions. Those emergency circumstances are such that there is probable cause that evidence relating to a crime will be found and an urgent and compelling risk of the destruction of evidence, the escape of a suspect or of a danger to the police officers or others. (*Kentucky v. King*, 2011) (*Brigham City, Utah v. Stuart*, 2006)

This particular exception to the requirement that the police obtained a warrant was not directly addressed by the holdings in *Wurie* and *Riley*. But it does implicate factual considerations that an emergency access to those event data recording devices would reasonably permit the preservation of evidence, the prevention of an escape of a suspect or the mitigation of danger to police officers or others.

One scenario raised in *Wurie* is that the cell phone might be used to summon individuals in support of the arrestee, presenting a danger to the officers. While the court dismissed that argument in that the arrestee no longer had possession of the cell

phone, it is possible that, depending on the circumstances, a cell phone may have immediate information relating to a warning to a suspect to flee, direction to destroy evidence or create a danger of injury to the police or others. If an officer can make the case that such evidence may be found in a device to support one of these conclusions, then a seizure and search without a warrant could be justified as an exigent circumstance. This may be as simple as checking a phone log to see who or what was called or texted immediately before an individual's encounter with the police. Examples where exigent circumstances may exist include the discovery or seizure of these devices in relation to an ongoing crime, such as a violent robbery, child abduction or the deployment of "weapons of mass destruction"; where there may be multiple criminal actors and an immediate risk of injury to others, the accessing of data showing immediate past activity and ongoing communications with others could be time critical for the prevention of death or injury.

3.3 Inventory Searches

The inventory search exception is built around policy principles of protecting the property of an arrestee as well as protecting state authorities from claims of damage or theft of property seized from an arrestee. (*Colorado v. Bertine*, 1987) It requires that there be defined and written limits on police discretion in searching and inventory search must be done pursuant to standard policies and procedures. Given the policy grounds for the protection of property and of the police from claims of damage to property, the reasoning in *Wurie* and *Riley* would indicate that the seizure and inventory search would be limited to the device itself and not permit an examination of the contents. To the extent of avoiding claims of damage the electronic information therein, the device could be placed in a protective bag; indeed, given the impact of search on a device and its contents it would be safer to not search the device as part of an inventory search absent a warrant.

3.4 Border Searches

Traditionally, anything can be searched crossing international borders; traditional Fourth Amendment protections did not apply, including as to computing devices.

But evolving case law within certain federal circuits, particularly the federal Ninth Circuit, have begun to limit that action absent "reasonable suspicion" of criminal activity (*United States v. Cotterman*, 2013) This reflects the same concerns as seen in *Wurie* and *Riley* that the sheer amount of information at issue may reduce the rights of intrusion and examination of devices that are collected such globally vast amounts of information. This doctrine will continue to evolve nationally and reflects the changing nature of technological systems for personal data recording, data encryption technologies and automated analytics of those devices.

This, too, reflects the radical change in both globalization of economies and portability of these powerful technological systems. Mandatory searches of computers and cell phones have been permitted where external information showed an individual had visited sites frequented for pedophilia sex tourism. But those devices might only contain personal information or trade and business secrets information unrelated to any crime but which are necessary for global activities. The trend does appear to require some facts that make it reasonable to intrude into these devices.

3.5 Investigative Detention (Terry Stop & Frisk)

One case law doctrine regards the ability of police to stop and "frisk" a subject on grounds less than probable cause that they have engaged in criminal activity. That standard,

similar to that adopted within the border search law, is that the police officer have a reasonable suspicion that criminal activity may be afoot and that, for the frisk, that the individual possesses a weapon. The extension in the case of data devices, again, might be a reasonable suspicion that a data device has been used in such a way as to create an immediate risk to an officer. This would be a greater extension of search rights that currently exist, and would seem to be contrary to the trend in greater data protection in data devices.

But this does fit within general investigative practices whereby the frisk does provide the officer with an additional bit of information regarding the subject, to wit, they have a cell phone. If that can be combined with other evidence it may lead to further actions by the police, such as extending the detention and questioning and, if sufficient information develops to establish probable cause, obtained a search warrant.

Practically, the discovery of the personal EDR device may lead to a police officer asking for consent to search the device, which a person may agree to under the stress of the moment.

3.6 Consent

Lastly, an investigative standby of great utility has been the consent search. Any individual may consent to the search of their data devices, regardless of whether a police officer has any suspicion of improper activity. It can be quite intimidating to have an officer asked to examine your device and have to make the decision as to whether to say yes or no to that request; indeed, there are many cases involving consent searches producing vast amounts of evidence of criminal activity. This particular exception also holds true for event data recorders of any kind. The one item to note is that once consent is given it may be withdrawn an individual can at that point terminate the search. But if an investigating officer has found evidence relating to criminal activity then, then the device may be seized for the preservation of evidence and, possibly, for actions under other exceptions to the search warrant requirement. But having once seized the device, if evidence of criminal activity is found then that should be sufficient for a presentation to a neutral magistrate to get a search warrant for the full examination of the device.

Table 2 summarizes possible changes in practice.

Table 2
Fourth Amendment issues with EDR

Exception	Requirements	Changes in lawful practice possible
Search Incident to Arrest	Contemporaneous with lawful arrest Limited to "grabbing space"	Yes
The "Automobile" Exception	Mobile vehicle, probable cause	Yes
Exigent Circumstances	Exigency, Objectively Reasonable Basis	Probably not
Inventory Searches	Lawful seizure	Probably not
Border Searches		Yes
Investigative Detention (Terry Stop)	Reasonable suspicion	Probably not
Consent	A legal consensual encounter	No

3.7 Collateral Civil Liability for Errors

There may be civil issues regarding liability for an invasion of privacy under both statutory protections and American common-law.

There have been efforts on a federal and state levels to provide notice to people that an event data recorder is present in recording specific types of information, which may be used in law enforcement proceedings and that the event data recorder in the data on it are the property of the owner of the automobile such that the retrieval of that information by any person anyone else is unlawful except with the owner's consent, a court order or the servicing of the vehicle by a dealer or automotive technician.

Some proposed protective legislation has not yet been enacted into law (H.R. 2414-Black Box Privacy Protection Act, US, 2013) Another proposed law establishes that the data in an EDR required to be installed under Department of Transportation regulations are the property of the owner or lessee of the vehicle and may not be accessed other than through a court or judicial/administrative order authorizing data retrieval according to law, the consent of the owner, retrieval Pursuant to Authorized Investigations of the National Transportation Safety Board or the Department of Transportation, pursuant to an appropriate for the emergency medical response in a motor vehicle crash or for traffic safety research where the owner or lessee's personally identifiable information and vehicle identification number or not disclosed (S.766 - Driver Privacy Act of 2015, US).

There may be the risk of civil liability for a digital forensics examiner looking at such data devices where the legal right to conduct such an examination has not been established. It continues to be a good practice to require documentation of a legal seizure and right to search of any particular medium for conducting the examination.

4. TRANSNATIONAL CONCERNS-RUSSIAN FEDERATION

Video event data recorders (VEDR) are widely deployed in the Russian Federation by everyday drivers, capturing images while driving, including before and after traffic

accidents. This is particularly valuable data that may be used for multiple purposes; in one case it was used for the diagnosis of an epileptic seizure that occurred in a taxi driver at the time of an automobile accident (Kotaro, et al. 2014).

When considering the issues raised in these technologies-legal, ethical, political-we may also look to how other governments approach these matters. Truth versus personal autonomy is, or should be, a matter of concern for all polities.

Police in the Russian Federation apply for electronic reception of documents and data in cooperation with other law enforcement agencies, state and municipal authorities, public associations and organizations.

Police utilize technical means such as audio, photo and video for documenting the circumstances of crimes, circumstances of accidents, including in public places (administrative offenses), as well as to monitor (register) the actions of police officers performing their duties (Art. 11) (On Police: Federal Law of 07.02.2011 N 3 –FZ of the Russian Federation).

In accordance with Art.2.6.7 of the Administrative Code of the Russian Federation administration of police use of special technical means is reflected in the record of an administrative offense or the judgment in the case of an administrative offense (Russian Federation Code of Administrative Offences of 30.12.2001).

Under Art. 2.6.1. of the Russian Federation Code of Administrative Offences administrative liability is enforced on the owners of vehicles for administrative violations in traffic and administrative violations in landscaping that are committed with the use of the vehicles. In these cases the recordation of activity of these administrative offenses is done by automatic mode using special means (event data recorders). These devices function through photographing and filming, recording, or by means of photography and filming, by the video recorders in vehicles.

The owner of the vehicle is exempt from administrative liability if, during the examination of the application for a ruling on the administrative case, it is established that at the time of recording of an administrative offense, his or her vehicle was in the possession or in use of another person or at that moment the owner was not in his or her possession as a result of wrongful acts of others at the time of an automobile accident.

Part 3, Article 6 of the Federal Law "On Operative-Investigative Activity" (OIA) is the legal grounds for secret (tacit) obtaining information about criminal activities (On Operative - Investigative Activities: Federal Law of 12.08.1995 of the Russian Federation). According to this clause, video and audio recordings, film and photography, as well as technical and other means are used in the course of search operation information systems, provided that they would not be harmful to life and health of people and cause no harm to the environment.

5. ETHICAL & PRACTICE ISSUES WITH EVIDENCE AND DIGITAL FORENSICS

The ethical issues raised by the data in these devices parallels the legal concerns but may also extend beyond legal limits. Under a Kantian perspective on ethics, the principles of equality and respect as applied to the private concerns of individuals give some direction.

An extreme example of the ethical concerns here addresses the publication of flight data recording and event data recording of the final, intimate moments of people-their last two

minutes of life- who are caught in a system failure that may lead to their deaths. (Bland 2015)

These issues reappear within the context of our modern data recording technologies. The ethical issues of the disclosure of information may be separate from the search from that information. Statutory regimes create different, separate liabilities for the use or disclosure of information, even where the acquisition of that information may be permitted. But even if there are no such prohibitions, it may not be good conduct to humiliate through the disclosure of information that serves no legitimate governmental purpose. In the extreme, this can invoke civil liability, but even before notions of liability we must consider the simple decency of actions both for their own good as well as an early warning system as possible conflicts with legal prohibitions.

One challenge to the fairness of prosecution has been the destruction of the sometimes volatile VEDR and EDR data where a defendant asserts it would have exculpated her or him. (*United States v. Gutierrez,* 2011) Although his argument failed, the federal Court of Appeals acknowledged that the Due Process Clause of the federal constitution imposes a duty on the government to preserve evidence; however, that duty is limited to evidence "that might be expected to play a significant role in the suspect's defense," and the government acted in bad faith, a proof burden that defendant was unable to meet. (*California v. Trombetta*, 1984) (*Arizona v. Youngblood*, 1988)

Another challenge introduced the practice and ethical requirement for forensic examination of the EDR. The defendant asserted trial counsel's failure to retain a forensic expert to contest the introduction of the Sensing and Diagnostic Module (SDM) and Event Data Recorder (EDR) evidence indicating the speed of defendant's vehicle at the time of collision constituted ineffective assistance of counsel and grounds for a new trial. (*Matos v. Secretary*, 2015) In affirming the court of appeals noted that the defendant had, in fact, had a forensic expert testify generally to the reliability of the SDM/EDR and that other evidence established his speeding as to render his claims insufficient.

VEDR/EDR forensic data provide valuable evidence in efforts at reliable fact-finding. It is essential that their use be by those ethical and competent in its analysis.

6. CONCLUSION

The issues regarding blackbox forensics will continue to evolve as device forensics generally. This is particularly the case as more and more devices become networked into systems for cloud storage of data, changing some of the forensic tasks necessary in these cases. And this will become increasingly complicated by the implementation of cryptographic technologies to preserve the privacy and confidentiality of data collected in the systems, for good or ill.

This will certainly be the case with aviation flight data recorders and flight data recording systems with the growing interest in real time satellite transmission of flight data in order to avoid the problems of lost flight data recorders manifested in the Malaysian Airlines flight 370 crash in the Indian Ocean and the Air France flight 447 in the Atlantic Ocean. Similar technologies are used now with some high-end automobiles.

The legal ramifications of the changing technology in our personal collection of our own personal data are slowly unfolding through both the case and statutory law. They are beginning to reflect an understanding of how even the simple localized retention of

personal data can significantly impact people's lives such that it is the deserving of protection. It is anticipated that this area will continue to undergo legal and policy development as we struggle with notions of personal autonomy and privacy, public and private security and the Internet-connectivity of everything in our lives.

REFERENCES

49 CFR Part 563, Table I (US).

Arizona v. Youngblood, 488 U.S. 51, 57-58, 109 S. Ct. 333, 102 L. Ed. 2d 281 (1988)

AutoGuard Dash Cam –Blackbox, Hovanoo, June 5, 2015

Batiste v. General Motors Corporation, 802 So.2d 686,687–88 (La.Ct.App.2001); *Harris v. General Motors Corporation*, 201F.3d 800,802(6thCir.2000).

Bierman, N. (2012) "Lt. Gov. Tim Murray was driving 100 mph at time of Nov. crash, may have fallen asleep at the wheel". *The Boston Globe*. January 3, 2012, accessed June 15, 2015

Bland, A., (2015) "German wings flight for you 9525: what's it like to listen to a blackbox recording?" The Guardian, 28 March 2015

Brigham City, Utah v. Stuart 547 U.S. 398, 126 S.Ct. 1943 (2006)

California Vehicle Code § 9951(c)(2) (US) (2015)

California v. Trombetta, 467 U.S. 479, 488, 104 S. Ct. 2528, 81 L. Ed. 2d 413 (1984).

Cnossen, R, Heetderks, W, Pettigrew, R., et al, (2015) "White Paper: Data Collection and Mobile Technologies" NIH Precision Medicine Meeting (2015) http://www.nih.gov/precisionmedicine/whitepapers/Data-Collection-Mobile-Technologies.pdf

Colorado v. Bertine, 479 U.S. 367, 107 S.Ct. 738 (1987)

Elmaghraby, A. & Losavio, Michael (2014) "Cyber Security Challenges In Smart Cities: Safety, Security and Privacy," Journal of Advanced Research 5, 491-497

H. R. 2414-Black Box Privacy Protection Act, 113th Congress (2013-2014) introduced June 18, 2013, amending the Automobile Information Disclosure Act of 1958 (US)

Kaste, M. (2014) Your Smart phone Is A Crucial Police Tool, If They Can Crack It," National Public Radio, March 25, 2014

Kentucky v. King, 563 U.S.__,131 S.Ct. 1849 (2011)

Losavio, M., Keeling, D, Lemon, M, (2012) " Models in Collaborative and Distributed Digital Investigation In the World of Ubiquitous Computing and Communication Systems," UNESCO International Conference on Memory of the World 2012, Vancouver, British Columbia, Canada

Matos v. Sec'y, Fla. Dep't of Corr 603 Fed. Appx. 763; 2015 U.S. App. LEXIS 2670 (10th Cir. 2015) (unpublished)

Mueller, P. (2006). Comment: Every Time You Brake, Every Turn You Make–I'll Be Watching You: Protecting Driver PrivacyInEventDataRecorderInformation,2006Wis.L.Rev. 135.

On Operative - Investigative Activities : Federal Law of 12.08.1995 N 144 -FZ (ed. By 12.21.2013 // Meeting of Legislators Assembly of the RF.1995 , N 33 , Art. 3349/

On Police: Federal Law of 07.02.2011 N 3 -FZ (ed. By 12.28.2013) // Federal Law of the Russian Federation . 2011, N 7, Art. 900

Paur, J. (2010) "March 17, 1953: The Black Box Is Born," Wired Magazine March 17, 2010

People v. Xinos (2011) 192 Cal.App.4th 637, 653- 654.)

Railway Technology, "HaslerRail -on On Board Train Monitoring and Recording Systems-Speed and Event recording," http://www.railway-technology.com/contractors/computer/hasler/, accessed June 23, 2015

Russian Federation Code of Administrative Offences of 30.12.2001 N 195 -FL (ed. By 29.06.2015 // the Russian Newspaper. 2001, issued on December 31

S.766 - Driver Privacy Act of 2015, 114th Congress (2015-2016) (US)

Sakurai, K., * Yamamoto, J., Kurita T., Youji T., & Kusumi, I. (2014), "Video event data recording of a taxi driver used for diagnosis of epilepsy" Epilepsy Behav Case Rep. 2014; 2: 24–25.

Sharp, D. (2003), "Autos' black-box data turning up in courtrooms". *USA Today*, May 15, 2003, accessed June 15, 2015

Smith, A., (2015) "U.S. Smartphone Use in 2015" Pew Research Center

http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/ (accessed July 9, 2015)

United States v. Cotterman, 709 F.3d 952,957 (9th Cir. 2013)(en banc*)*

United States v. Gutierrez, 415 Fed. Appx. 870; 2011 U.S. App. LEXIS 2801 (10th Cir. 2011) (unpublished)

United States v. Jones, 565 US, 132 S Ct 945 (2012)

