

Presentation to IEEE P1616 Working Group on MVEDR

AVAILABILITY AND ACCESSIBILITY OF MVEDR DATA

Roger L. Boyell

29 April 2002

1. Basis for these comments
 - A. Analyze equipment operating, or failing, in the physical world
 - B. Recognize the potential of MVEDR for scientific data retrieval
 - C. Concern about proprietary protocols and secrecy provisions
2. NHTSA EDR Working Group reported (August 2001)
 - A. Database/retrieval systems suit various organizations' own interests
 - B. Generally proprietary or confidential and not accessible by public
 - C. Differing needs of manufacturer, owner, operator, court, insurer, etc.
3. Other data systems balance competing interests
 - A. Consumer credit information
 - B. Medical history
 - C. Vehicle diagnostic codes
 - D. Facial recognition
4. Proposed MVEDR availability and accessibility policy
 - A. Aggregate data, without any individual identifiers, is widely available (government, manufacturers, safety organizations, advocacy groups)
 - B. Individual/personal data accessible only to those directly affected (owner, operator, lessor, involved persons by appropriate court order)
 - C. Data recovery schemes preserve all rights in the data, including the rights of data owners and adversaries to dispute the evidentiary weight
5. Some situations may demand exposure of individual/personal data.
 - A. Crash victim claims EDR will show a specific vehicle defect
 - B. Law enforcement uses EDR to prove/exculpate a traffic violation
 - C. High-profile civil damage suit is resolved only through EDR data
 - D. EDR's permit an insurance carrier's investigation of staged crashes
 - E. A court rules on a party's intentional spoliation of EDR evidence

6. Authenticity of recovered individual/personal data must be assured
 - A. Aggregate data may contain an occasional statistical anomaly or loss. While scientifically undesirable, minor errors are not catastrophic.
 - B. But individual/personal data with errors or omissions may wrongly attribute liability, falsely indicate fraud, or convict an innocent person.

7. Public acceptance
 - A. Fear of MVEDR monitoring will tend to dissipate when the collected and recovered information is readily available to the authorized user for his review and evaluation (e.g. consumer credit information, vehicle diagnostic codes).
 - B. The legal community will embrace MVEDR's if the data is made accessible and its interpretation scientifically recognized (e.g., DNA).

8. Conclusions
 - A. Individual/personal MVEDR data can have significant forensic value
 - B. MVEDR's should provide for full data disclosure to those authorized
 - C. Incentives abound to tamper with individual/personal MVEDR data
 - D. MVEDR standards should address preservation of data authenticity

9. Recommendations
 - A. Avoid proprietary protocols and special data formats
 - B. Restrict unique recording and secret playback mechanisms
 - C. Promote wide availability and accessibility of MVEDR data
 - D. Incorporate means to prevent, or at least to detect, data tampering
 - E. Establish methods and standards for data recovery, readout, and display as an integral part of the MVEDR standardization process

MVEDR data might be as crucial to an involved individual as his own DNA profile. His relevant MVEDR data should be accorded a correspondingly privileged status.

ROGER L. BOYELL, FORENSIC ANALYST
416 PARRY DRIVE, MOORESTOWN NJ 08057-2877
PHONE 856-234-5800 • FAX 856-234-9539
E-MAIL boyell@ieee.org • WEB SITE www.boyell.com