

Criminal Law News



THOMSON REUTERS

Contents -

Criminal Law News, Issue

Drink, Drugs and Driving	pgs 2-9
Protection of Freedoms Act	pg 10
Data hijacking	pgs 11-12
Intellectual Property, Customer Information and Employee Information stolen	pgs 12-13
Effective use of data can reduce fraud	pgs 13-14
DVD piracy alive and well in the UK	pgs 15-16

- Chief Editor: Sally Ramage, Member of the Chartered Institute of Journalists; Society of Editors and Society of Legal Scholars, UK.
- Consultant Editors: Dr Nicholas Ryder, Reader in Law, Head of Commercial Law Research Unit, University of the West of England, UK.
David Selfe, Director, Law School, Liverpool John Moores University, UK.
Joanne Clough, Solicitor and Senior Lecturer at Northumbria Law School, Newcastle-Upon-Tyne, UK.
Roderick Ramage, Consultant Solicitor at Weightmans, LLP
Edward S. A. Wheeler, Principal Desktop IT Manager, Medway Council, UK.
- Design: David. E. Tonkinson, Designer and Online Editor, Poole, UK.

Drink, Drugs and Driving

Sally Ramage

This article will reveal the potential inadequacies of police equipment; potential corruption; and the consequences of the rule of law. It compares the incidents of drink-and drug-driving in the United States and the United Kingdom.

Drugged drivers

It has been reported by Gil Kerlikowske, United States (U.S.) Director of National Drug Control Policy, (NDCP) Washington D.C., that statistics reveal that one in three fatally injured drivers tested positive for drugs. ‘Traffic fatality analysis’ by the U.S. police revealed that this high percentage of drivers killed (33%) had drugs in their system, according to blood tests. Worryingly, the percentage of victims who showed positive readings for drugs in their system has increased, even as the total number of road vehicle crashes is decreasing. Kerlikowske drew attention to the alarmingly high percentage of fatalities on United States roadways involving drivers that had drugs in their system and called on communities to act immediately to prevent drug use in light of this new traffic fatality analysis, released by the National Highway Transportation Safety Administration (NHTSA).

U.S. Fatal Accident Reporting System

Note that the U.S. national data, which focuses on the danger of driving under the influence of alcohol, is readily available and often cited, but less is known or discussed about drivers under the influence of other drugs. This is the first analysis of drug involvement from NHTSA's Fatal Accident Reporting System (FARS) census.

Drugs consumed by fatally injured drivers

The detailed result of this first drug-driving census showed that:- one in three motor vehicle fatalities with known drug test results tested positive for drugs in 2009. In addition, the involvement of drugs in fatal crashes has increased by five percent over the past five years, even as the overall number of drivers killed in motor vehicle crashes in the United States has declined.

Better tools to detect the presence of drugs

Drug-taking drivers are a much bigger public health threat than most people realize and it may be getting worse, said Kerlikowske. The director said that communities across the U.S. must address the threat of drugged driving in order to make U.S. roadways safer. This can be achieved by increasing public awareness, employing more targeted enforcement, and developing better tools to detect the presence of drugs among drivers.

These new data from the NHTSA census reports that the fatally injured drivers (over

the years 2005-2010) had the following drugs in their blood:

narcotics; depressants; stimulants; cannabinoids (marijuana); hallucinogens; anabolic steroids; and inhalants.

Gross misdemeanour

The analysis could not reveal whether legal medications had been misused. Drugs recorded in FARS included: alcohol; nicotine; and aspirin. Note that Washington's DUI laws state that 'driving under the influence' is a gross misdemeanour.

Driving Under the Influence (DUI)

A person is guilty of Driving under the Influence when:

'(1) under the influence of intoxicating liquor or any drug if the person drives a vehicle,

(a) and the person has, within two hours after driving, an alcohol concentration of 0.08 or higher as shown by analysis of the person's breath or blood made under RCW 46.61.506; or

(b) while the person is under the influence of or affected by intoxicating liquor or any drug; or

(c) while the person is under the combined influence of or affected by intoxicating liquor and any drug.

(2) The fact that a person charged with a violation of this section is or has been entitled to use a drug under the laws of a state shall not constitute a defence against a charge of violating this section.

(3) It is an affirmative defence to a violation of subsection (1) (a) of this section if the defendant proves by a preponderance of the evidence, that he or she consumed a sufficient quantity of alcohol after the time of driving and before the administration of an analysis of the person's breath or blood to cause the defendant's alcohol concentration to be 0.08 or more within two hours after driving. The court shall not admit evidence of this defence unless the defendant notifies the prosecution prior to the omnibus or pre-trial hearing in the case of the defendant's intent to assert the affirmative defence.

(4) Analyses of blood or breath samples obtained more than two hours after the alleged driving may be used as evidence that within two hours of the alleged driving, a person had an alcohol concentration of 0.08 or more in violation of subsection (1)(a) of this section, and in any case in which the analysis shows an alcohol concentration above 0.00 may be used as evidence that a person was under the influence of or affected by intoxicating liquor or any drug in violation of subsection (1)(b) or (c) of this section.

(5) A violation of this section is a gross misdemeanour.'

Washington DC: breath analysers at issue

Added to this issue is the fact that, since 2010, the city's breath testing equipment has been in dispute by defence attorneys after some machine results were found to be inaccurate, resulting in the Medical Examiner of Washington D.C. being unable to verify the accuracy of machine readings from all Intoxilyzer 5000 police equipment. The Intoxilyser was then replaced by another machine in March 2011: the Intoximeter.

Equipment readings not evidence

In one case, D.C. Attorney General Irvin Nathan was forced to drop the drink and drug driving charges against several suspects. The police procedure in Washington D.C. is that the medical examiner's office must certify the breathalyser program, and it has not been able to do so due to concerns raised by the problems with the previous models of the breathalyser equipment.

Police officers are still using the newer equipment, *the Intoximeter*, but at present, these readings are not being used in evidence in court. Instead, urine sample readings of blood-alcohol levels are used in evidence. Many DIU charges have been quashed to comply with the U.S. 6th Amendment to the Constitution:

'In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the state and district wherein the crime shall have been committed, which district shall have been previously ascertained by law, and to be informed of the nature and cause of the accusation; to be confronted with the witnesses against him; to have compulsory process for obtaining witnesses in his favour, and to have the assistance of counsel for his defence.'

Lawsuits against Medical Examiner's Office

There are many lawsuits being brought against the medical examiner by convicted drivers. Analysis has revealed that the majority of drink-driving charges were brought

by only two of the city's police officers and this revelation has led to an internal police investigation. Inevitably, the city's police force has been demoralised because it cannot enforce DUI laws.

The United Kingdom's progress in this road traffic offense

In the United Kingdom, no-one has challenged the incompetence of the breath-testing road-side machine that road traffic police use. The UK Road Traffic Act 1988, section 4 (1) deals with the offence of being 'unfit through drink or drugs'. Section 4 (1) states:

'A person who, when driving or attempting to drive a mechanically propelled vehicle on a road or other public place, is unfit to drive through drink or drugs is guilty of an offense.

This offense is triable summarily and the punishment is six months imprisonment and/or a fine and obligatory driving disqualification. Note that section 4 creates three separate offences, giving definitions for 'driving'; 'attempting to drive' and 'in charge of a vehicle'.

Although there was much talk of road police having a new machine to detect drugs in a driver, it has not yet come about. Rather, there is a long-winded and rather subjective way of prosecuting for driving under the influence of drugs and there is not yet even a list of which 'drugs' are prohibited. As regards equipment testing for alcohol consumption, however, an important issue has been 'failure to comply with the equipment manufacturer's instructions on the use of approved devices. In the past the Divisional Court decided that an 'innocent' failure by a police officer to follow the

manufacturer's instructions should not be deemed to render the breath test of subsequent arrest unlawful. (See *DPP v Kay* [1999] RTR 109).

Code of Guidance for observation evidence

A preliminary impairment test under section 6B must involve an appropriately trained and authorised police officer observing the driver performing specified tasks and that police officer must make evidence of his observations. The Secretary of State has set out a *Code of Guidance* for such observations. This includes:

pupillary examination;

walk-and-turn tests;

finger-to-nose tests.

Objective cause of police officer's belief

Refusal to comply with these tests means failure in the tests and immediate arrest.

(UK Road Traffic Act 1988, section 6(6)). Although the police officer uses 'reasonable cause' to believe that medical testing should be done, it is the *objective cause* of that belief that is considered by the courts. (See *Jubb v DPP* [2002] EWHC 2317).

Police can randomly stop drivers but the law does not permit entirely random testing of drivers for drink or drugs (UK Road Traffic Act 1988, section 163). The police cannot interview a stopped driver unless he is first cautioned. The police can suspect that a driver has been drinking alcohol merely from the smell of his breath, after which he or she will caution the driver and require a roadside breath test.

No definition of uniformed officer

If the road police suspect that the driver is under the influence of drugs, the law in section 6A, 6B and 6C, provide for a roadside test of a specimen of sweat or saliva. Section 6C provides for the police to take the driver to the nearest police station where a preliminary drug test may be administered. This drugs test must be administered by a police officer in uniform (section 6 (7)). The word ‘Uniform’ is not defined but police look to a 1970 precedent caselaw (*Wallwork v Giles* [1970] RTR 117).

Doctor may take samples of blood and urine

The legislation states that the driver’s own doctor cannot take these samples. Section 7 A (6) states that refusal to allow these samples to be taken is triable summarily, being automatically guilty of an offense.

Hundreds of deaths in police custody

It is to be noted that some 200 persons die in police custody, many of whom find themselves there because they are thought to be drunk. Of 333 published deaths in UK Police custody, there were 7 prosecutions of police of which only one police officer and one staff member were found guilty of ‘misconduct in public office’. (Police were exempted from the law of the UK Corporate Manslaughter Act 2007).

References

Freeman Kloppot, ‘D.C. attorney general drops drink driving cases’, *Washington*

Examiner, 25.2.2011. See <http://washingtonexaminer.com/local/dc/2011/02/dc-attorney-general-drops-drunken-driving-cases>

‘Police Reform and Social Responsibility Act 2011’ Comment by Sally Ramage

Protection of Freedoms Act 2012

Comment by

Sally Ramage

The Protection of Freedoms Act 2012 provides for the destruction, retention, use and other regulation of certain evidential material; imposes consent and other requirements in relation to certain processing of biometric information relating to children; provides for a code of practice about surveillance camera systems and for the appointment and role of the Surveillance Camera Commissioner; provides for judicial approval in relation to certain authorisations and notices under the Regulation of Investigatory Powers Act 2000; provides for the repeal or rewriting of powers of entry and associated powers and for codes of practice and other safeguards in relation to such powers; makes provision about vehicles left on land; provides for a maximum detention period of 14 days for terrorist suspects; replaces certain stop and search powers ; provides for a related code of practice; amends the Safeguarding Vulnerable Groups Act 2006; makes provision about criminal records; disregards convictions and cautions for certain abolished offences; makes provision about the release and publication of datasets held by public authorities and to make other provision about freedom of information and the Information Commissioner; and repeals certain enactments.

Data hijacking

Sally Ramage

A number of large corporations have suffered computer hijacking. Such data security breaches and corporate data theft are very serious incidents, reminding all companies of all sizes to review their data security. Regulators are beginning to attend to this matter also, bearing in mind that legislation, especially U.S. legislation, makes it obligatory for such corporate data breaches to trigger a ‘Breach Notification Obligation’.

Any unauthorized acquisition of [unencrypted] computerized data must be notified by the affected corporation to shareholders and investors including institutional investors. The timeframe for notifying parties is ‘in the most expedient time possible and without unreasonable delay.’

In the United States, such data breach must be reported to third parties ‘in writing (on paper and sent by mail); in electronic form (by e-mail, but only if the individual has consented in advance to receiving the notice in electronic form); by substitute notice; by telephone (in certain countries-(note that in the United States (the states of Montana, New York and North Carolina) notification of data breaches may be performed by telephone. At the same time, certain states do not permit notification of data breach to be performed by email.

Inter-agency Guidance

Customer notice should be delivered in any manner designed to ensure that a customer can reasonably be expected to receive it. For example, the institution may choose to contact all customers affected by telephone or by electronic mail for those customers for whom it has a valid e-mail address and who have agreed to receive communications electronically.

The problem is that business owners typically have a false sense of security and in fact, most business owners believe their company is safe from hackers, viruses, malware or a cyber-security breach, according to a September 2012 survey of over 1,000 U.S. small businesses sponsored by Symantec Corp. Symantec Corp. This is particularly true of small and mid-sized businesses (SMBs) that don't consider themselves targets, said Maxim Weinstein, executive director of StopBadware, a non-profit organization that provides online tools and information on how to protect against malware.

As large enterprises put strong defences in place, cyber-criminals move down the line to where there is opportunity, ie to the smaller businesses. Customer data, intellectual property and banking credentials are all valuable to criminals, no matter the size of the organization. A loss of intellectual property, critical data and money cripples many SMBs each year

Opportunistic data threats

The bulk of opportunistic security threats can be prevented by doing three things: Keeping software up to date, using the most current versions of antivirus software and training your employees about data security practices. While these sound like simple solutions, some of the most basic data security practices are not put in place and many businesses lack sufficient cyber security policies and training. Discussions about staying safe online and securing company assets simply are not happening and in fact, 77 percent of business owners said in a NCSA survey that they do not have a formal written Internet security policy for employees and of those, 49 percent reported that they do not even have an informal policy. In addition, 56 percent of businesses do not have Internet usage policies that state what websites and web services employees may use. It is in no way a draconian measure if at the very least, businesses have policies that provide legal protection and set expectations.

Intellectual Property, Customer Information and Employee Information stolen

Sally Ramage

There are many reported cases of data theft and it is clear that business owners of all sizes need to take the time to protect their data and thus avoid becoming a victim. The first step to creating a data security plan is to understand what is at risk. Intellectual property, customer information and employee information are all ‘the coin of the realm’ for cyber-criminals and these assets must be protected.

Strong Passwords

One of the simplest ways to protect sensitive data is by using strong passwords. A strong password would incorporate a combination of letters, both upper and lowercase, numbers, and punctuation marks.

Install antivirus software

To protect against malware, employers must install antivirus software and keep such software up- to -date. Implementing policies around the types of websites and data which employees access while on a corporate network is essential. Because of the abundant use of smart-phones or tablets at work, businesses must set some clear policies surrounding data access on mobile devices and secure email practices. For instance, sensitive customer information or intellectual property data should not be installed on devices that run the risk of being lost or stolen.

Encryption

It's also good practice to encrypt data that is accessed on mobile devices and to set up a way to remotely wipe sensitive data in case a device is lost or stolen

Effective use of data can reduce fraud

Sally Ramage

Fraud, errors and debt costs the government an estimated £31 billion per year. To reduce fraud and error, the government needs to make effective use of data, so that it

can identify when public money is being misappropriated. The government can therefore prevent people from abusing the public purse. There have been many cases of fraudulent claims for tax credits to the sum of millions of pounds from Her Majesty's Revenue and Customs ('HMRC') and one way of reducing this is simply to check whether all claims that purport to be single parents are indeed so, by analysis of data to show financial dependence. HMRC can then make an evidence-backed decision to adjust that claimant's benefit amount, to reflect their true circumstances. Another analysis that HMRC can use is to analyse claimants spending habits to find discrepancies in declared income. Were there data sharing (specifically for the purpose of analysis only) between government agencies, more would be revealed. It has been revealed that HMRC used such analysis in a pilot project that saved the government £19.5 million in a few months, and projected, this can result in a government saving of £2 billion over three years. However, this saving includes repayment of monies incorrectly claimed, which may mean that the government will use debt collectors' services.

DVD Piracy-alive and well in the UK

Sally Ramage

When in 2006, newspapers reported such crimes as the report below, many thought that, eight years on, Trading Standards and the Police would have been able to bring the Intellectual Property Law crime to a halt. But it thrives as ever.

Five people have been arrested in a police raid on what is thought to be the largest DVD piracy factory discovered in the UK. The Metropolitan Police's film piracy unit found more than 60 DVD copying machines and 30,000 blank discs in the search of the east London premises. A factory in an industrial estate in Leyton was capable of producing 2,700 DVDs an hour. A large number of printed cover inlays were also

found. The raid was a joint operation between the film piracy unit, trading standards and the Federation Against Copyright Theft (Fact).'



Printed and published by Sally Ramage@. Copehale, Coppenhall, Stafford, ST18 9BW, UK. Registered as a Newspaper at the Post Office. © Sally Ramage® 2013. All Rights Reserved. No part of this publication may be reproduced in any material form (including photocopying or storing it in any medium by electronic means and whether or not transiently or incidentally to some others use of this publication) without the written permission of the copyright holder except in accordance with the provisions of the Copyright, Design and Patents Act 1988 or under the terms of a licence issued by the Copyright Licensing Agency, Saffron House, 6-10 Kirby Street, London, England EC1N 8TS. Application for the copyright owner's written permission to reproduce any part of this publication should be addressed to the publisher. Warning: the doing of an unauthorised act in relation to a copyright work may result in both a civil claim for damages and criminal prosecution. ISSN1758-8421.