



STATE BAR OF MICHIGAN

Michigan IT Lawyer

A Publication of the State Bar of Michigan Information Technology Law Section

<http://www.michbar.org/computer>

Table of Contents

January 2011 ■ Vol. 28, Issue 1

- Bits and Bytes from the Chair 1
- *U.S. v. Herring*: Are Errors in Government Databases Preventing Defendants From Receiving a Fair Trial? 2
- Publicly Available Websites for IT Lawyers 14
- Meet a Section Member: Jeanne Moloney 15
- 2011 Edward F. Langs Writing Award ... 16
- Mission Statement—Information Technology Law Section, State Bar of Michigan 16

Bits and Bytes from the Chair

By Mark G. Malven, *Dykema Gossett PLLC*

As your Chair I wanted to let you know we have a couple of interesting events coming up, and I encourage all to attend:

On the evening of March 10, in conjunction with our next Council Meeting at Wayne State University Law School, our IT Law Section will be sponsoring what I believe will be a very interesting presentation. Professor (and Associate Dean) John Rothchild has graciously agreed to speak on the currently hot topic of “Net Neutrality.” Professor Rothchild is a recognized expert in IT Law and is a co-author of “Internet Commerce,” a law school casebook published by Foundation Press, which has been adopted for classroom teaching at more than 30 law schools. Prior to his time in academia, Professor Rothchild was an attorney at the Federal Trade Commission’s Bureau of Consumer Protection, specializing in law enforcement efforts addressing Internet-based fraud and online compliance issues, and for several years he led the Commission’s international consumer protection program.

On the evening of April 21, our IT Law Section will be co-sponsoring a networking event at the Post Bar in Novi. This is a reprise of our successful spring networking event last year in conjunction with DetroitNET.org. In case you are not familiar, DetroitNET.org is one of the largest networking groups for IT professionals in the region. Last year was great fun and this will be a can’t-miss event.

As always, if you have any suggestions, comments etc. for how we may be of service to you as a member of the IT Law Section, please do not hesitate to contact me.

Best regards,

Mark Malven

Michigan IT Lawyer is published every other month. Previously published issues of the *Michigan IT Lawyer*, and its predecessor the *Michigan Computer Lawyer*, are available at <http://www.michbar.org/computer/newsletters.cfm>. If you have an article you would like considered for publication, send a copy to:

Michael Gallo
2700 Renshaw Drive
Troy, Michigan 48085
e-mail: michael@gallo.us.com





2010-2011

Information Technology Section Council

Chairperson ▪ Mark G. Malven
Chairperson-elect ▪ Charles A. Bieneman
Secretary ▪ Karl A. Hochkammer
Treasurer ▪ Ronald S. Nixon

COUNCIL MEMBERS

Charles A. Bieneman
Susanna C. Brennan
William Cosnowski, Jr.
Nilay Sharad Davé
Jeanne M. Dunk
Samuel J. Frederick
Michael Gallo
Brian A. Hall
Karl A. Hochkammer
William J. Lamping, Jr.
Mark G. Malven
Tatiana Melnik
Ronald S. Nixon
Carla M. Perrota
Vincent I. Polley
Claudia Rast
David R. Syrowik
Mary Ann Wehr

Immediate Past Chair

Jeremy D. Bisdorf

Ex-Officio

Claudia V. Babiarz
Thomas Costello, Jr.
Kathy H. Damian
Christopher J. Falkowski
Robert A. Feldman
Sandra Jo Franklin
Mitchell A. Goodkin
William H. Horton
Lawrence R. Jordan
Charles P. Kaltenbach
Michael S. Khoury
J. Michael Kinney
Edward F. Langs*
Thomas L. Lockhart
Janet L. Neary
Kimberly A. Paulson
Paul J. Raine*
Jeffrey G. Raphelson
Frederick E. Schuchman III
Steven L. Schwartz
Carol R. Shepard
Anthony A. Targan
Stephen L. Tupper

Commissioner Liaison

Richard J. Siriani

Newsletter Editor

Michael Gallo

*denotes deceased member

The *Michigan IT Lawyer* is pleased to present “U.S. v. Herring: Are Errors in Government Databases Preventing Defendants From Receiving a Fair?” by Alex R. Hess. Mr. Hess is one of three student authors to receive a 2010 Edward F. Langs Writing Award from the State Bar of Michigan’s Information Technology Law Section. The statements made and opinions expressed in this essay are strictly those of the author, and not the State Bar of Michigan or the Information Technology Law Section. Comments regarding this article can be forwarded to the *Michigan IT Lawyer*, care of michael@gallo.us.com. Enjoy!

U.S. v. Herring: Are Errors in Government Databases Preventing Defendants From Receiving a Fair

By Alex R. Hess¹

Hypothesis

Herring v. United States will result in unfair criminal trials through the use of evidence obtained by Fourth Amendment violations due to numerous errors in government databases containing incorrect criminal records.

Abstract

Technology and invention has forced the Court to modify the rule of law to keep up with American ingenuity and innovation. While one’s mind often goes to the intellectual property field, technology may also have far-reaching implications in the criminal justice arena. In the modern age, where law enforcement is dependent on computers, the accuracy of government databases may determine whether a defendant gets a fair trial.

Technology has played a major role in the area of Fourth Amendment search and seizure law through its use in law enforcement and the determination of probable cause. In 1961, *Mapp v. Ohio* applied the Exclusionary Rule to all federal and state criminal proceedings; suppressing evidence at trial that was obtained through a Fourth Amendment violation. However, since *Mapp*, the Supreme Court has limited the application of the Exclusionary Rule. When probable cause for an arrest is founded on errors in government databases, the Supreme Court has allowed evidence obtained from that search into trial [*Arizona v. Evans*, 514 U.S. 1]. As a result, individuals are having their Fourth Amendment rights violated during the illegal seizure, and when that evidence is introduced at trial.

The most recent decision of *Herring v. United States* even further restricts the application of the Exclusionary Rule where errors in government databases form the basis for a search [*Herring v. United States*, 129 S. Ct. 695]. Under *Herring*, errors in government databases have the potential to infringe on an individual’s

right against unreasonable search and seizures. The result is unfair: the accused is faced with illegally seized evidence and the government receives no penalty for keeping incorrect records. As policing becomes more reliant on computerized systems, the number of illegal arrests and searches based on errors in government record-keeping is poised to multiply. Prosecutors, defense attorneys and judges will begin to see dramatic changes in Fourth Amendment jurisprudence.

Introduction

In 1791, the framers of our Bill of Rights could not have foreseen the technological advancements that came about during the modern age.² As Justice Brandeis put it “this Court has repeatedly sustained the exercise of power by Congress, under various clauses of the Constitution, over objects of which the Fathers could not have dreamed.”³ Marvel and invention have redefined law enforcement in both the field and in the courtroom. In response, the judiciary has been forced to balance the rights of the accused with those of law enforcement.⁴ The ever-changing technology used by police and prosecutors has made it difficult to establish bright line rules regarding evidence obtained through the use of technology.⁵ Thus the legal landscape surrounding technology and the Fourth Amendment is also ever-changing.⁶

In the modern age, where law enforcement is dependent on computers, the accuracy of government databases may determine whether a defendant gets a fair trial. Technology has played a major role in the area of Fourth Amendment search and seizure law through its use in law enforcement and the determination of probable cause. In 1961, *Mapp v. Ohio* applied the Exclusionary Rule to all federal and state criminal proceedings; suppressing evidence at trial that was obtained through a Fourth Amendment violation. However, since *Mapp*, the Supreme Court has limited the application of the Exclusionary Rule. When probable cause for an arrest is founded on errors in government databases, the Supreme Court has allowed evidence obtained from that search into trial [*Arizona v. Evans*, 514 U.S. 1]. As a result, individuals are having their Fourth Amendment rights violated during the illegal seizure, and when that evidence is introduced at trial.

The most recent decision of *Herring v. United States* even further restricts the application of the Exclusionary Rule where errors in government databases form the basis for a search [*Herring v. United States*, 129 S. Ct. 695]. Under *Herring*, errors in government databases have the potential to infringe on an individual’s right against unreasonable search and seizures. The result is unfair: the accused is faced with illegally seized evidence and the government receives no

penalty for keeping incorrect records. As policing becomes more reliant on computerized systems, the number of illegal arrests and searches based on errors in government record-keeping is poised to multiply.

History

The Exclusionary Rule and Early Technology

In 1914, The Supreme Court unanimously ruled that evidence seized in violation of the Fourth Amendment must be excluded from evidence in federal criminal prosecutions.⁷ This remedy, known as the Exclusionary Rule, provides a disincentive to police officers and prosecutors who illegally gather evidence in violation of the Fourth Amendment.⁸ The *Weeks* Court recognized that unless a remedy was available to those who have had their rights violated, the Fourth Amendment protections would mean nothing:

The Fourth Amendment was intended to secure the citizen in person and property against unlawful invasion of the sanctity of his home by officers of the law acting under legislative or judicial sanction. This protection is equally extended to the action of the Government and officers of the law acting under it. To sanction such proceedings would be to affirm by judicial decision a manifest neglect if not an open defiance of the prohibitions of the Constitution, intended for the protection of the people against such unauthorized action.⁹

While the *Weeks* decision significantly changed criminal procedure and increased the protections under the Fourth Amendment, its holding did not extend to state criminal proceedings.¹⁰ This limitation, lasted four decades, until a change in court membership brought with it a change in judicial philosophy.¹¹ The Warren Court dramatically reformed criminal procedure through incorporating the Bill of Rights and its protections to apply to state criminal proceedings.¹²

In 1960, after receiving a tip that Dollree Mapp was harboring a fugitive at her home, the Cleveland police broke into her home flashing a fake warrant in her face, when in fact they did not have a search warrant.¹³ After an exhaustive search of the house, the police discovered obscene material that violated Ohio anti-obscenity statutes.¹⁴ The *Mapp* Court was troubled by this deliberate violation of the Fourth Amendment and held that the evidence seized must be excluded from the state criminal proceeding.¹⁵ While *Mapp* drastically expanded the reach of the exclusionary rule, twenty years later the membership of the Supreme Court had changed, and once again, so had the philosophy of the majority.

In 1984, the Supreme Court curtailed application of the exclusionary rule by creating a “good faith” exception.¹⁶ In California, police officers executed a search warrant that was later invalidated due to a lack of probable cause.¹⁷ In holding that the evidence obtained through the search is admissible at trial, the *Leon* Court reasoned that the purpose of the exclusionary rule is the deter police misconduct, and that excluding the evidence here would not deter the judiciary from issuing unsound warrants.¹⁸ In limiting the reach of the exclusionary rule, the *Leon* Court stated “Suppression of evidence obtained pursuant to a warrant should be ordered only on a case-by-case basis and only in those unusual cases in which exclusion will further the purposes of the exclusionary rule.”¹⁹

A decade later, the Supreme Court once again narrowed the exclusionary rule when it had to determine whether suppression of evidence is appropriate when police conduct a search based on an error in a government database.²⁰ When police officers stopped Isaac Evans for a traffic violation, a computer check revealed an outstanding arrest warrant.²¹ When officers arrested Evans, a search of his vehicle following the arrest revealed a bag of marijuana under the driver seat.²² As it turned out, the arrest warrant had been revoked seventeen days before the arrest, but the court that quashed the warrant never informed the police and their database was never updated.²³ Isaac Evans appealed his conviction on the grounds that the drug evidence was the “fruit of an unlawful arrest” and that the marijuana should be suppressed because “the purposes of the exclusionary rule would be served here by making the clerks ... more careful about making sure that warrants are removed from the records.”²⁴ The Arizona Supreme Court reversed Evans’s conviction, and held that suppressing the marijuana would “serve to improve the efficiency of those who keep records in our criminal justice system.”²⁵

Ultimately, however, the Supreme Court disagreed and *Arizona v. Evans* extended the good-faith exception to the exclusionary rule to apply to government database errors. In reaching this conclusion, the *Evans* Court stated that “the exclusionary rule was historically designed as a means of deterring police misconduct, not mistakes by court employees.”²⁶ More importantly, the *Evans* Court relied on the fact that there is no basis for believing that applying the exclusionary rule to court clerk errors would increase the accuracy of police databases.²⁷

Government Databases and Errors

In 1967, FBI director J. Edgar Hoover created the National Crime Information Center (“NCIC”) to facilitate information flow between the numerous federal and state branches

of law enforcement.²⁸ The NCIC is a computerized database that provides access to information about criminals, their records and missing persons to law enforcement agencies.²⁹ Data on criminal records, wanted persons and crimes are exchanged throughout federal and state law enforcement agencies and ultimately compiled into the FBI’s NCIC database.³⁰ The NCIC is the nation’s largest criminal database, and provides over 80,000 law enforcement agencies, including police departments, with access to data on wanted persons, missing persons, gang members as well as information on stolen items.³¹

By 1974, the NCIC’s importance and influence over law enforcement caused Congress to act and regulate the database.³² The Privacy Act of 1974 (“Privacy Act”) requires government agencies to keep accurate records.³³ This applied both to the NCIC database and to local databases held by federal and state agencies.³⁴ Upon inception of the NCIC, the accuracy of these records was at issue and certain courts made their position on the matter known.³⁵ Most notably was the U.S. Circuit Court of Appeals for the District of Columbia:

The FBI cannot take the position that it is a mere passive recipient of records received from others, when it in fact energizes those records by maintaining a system of criminal files and disseminating the criminal records widely, acting in effect as a step-up transformer that puts into the system a capacity for both good and harm.³⁶

From 1971-1984, during his time as executive director of the ACLU’s Washington office, John Shattuck was at the forefront of major civil rights and liberties issues during the Nixon, Ford, Carter and Reagan administrations, often involving the accuracy of government databases.³⁷ In New Orleans, a mother on welfare was arrested and jailed for eighteen hours on the basis of an inaccurate crime report resulting from programming errors in police computers.³⁸ In New York, a middle-aged man was denied a license to drive a taxi because a computerized credit report showed that when he was thirteen years old in Massachusetts he temporarily had been placed in a mental institution, but the file failed to show that he was an orphan and the institution was the only home the state authorities could find for him for a period of four years.³⁹ In Ohio, five employees of a clothing store were fired and the employer spread reports that the employees had been stealing, although none were ever charged with theft.⁴⁰ These instances are a few examples of how errors in government databases have disrupted the lives of individuals, and how serious criminal consequences may result.

According to the Electronic Privacy Information Center (“EPIC”), numerous reports indicate that government databases are filled with errors.⁴¹ In both a 1997 report and a 2002 follow-up report, the Inspector General of the Department of Justice found that data from the Immigration and Naturalization Service was unreliable and “seriously flawed in content and accuracy.”⁴² However, due to recent actions taken by the Department of Justice (“DOJ”), little can be done to remedy these errors.⁴³

The bite of the Privacy Act has been severely lessened over the years by the numerous exemptions granted to certain agencies by the DOJ.⁴⁴ One notable exemption is the Department of Homeland Security, who sought and received in 2003 an exemption from the requirement that the agency assure the reliability of their databases.⁴⁵ In 2003, the DOJ exempted the FBI of its statutory duty to ensure accuracy and completeness of over 39 million criminal records maintained by the National Crime Information Center (“NCIC”).⁴⁶ In response to this exemption, EPIC launched a campaign to reestablish the accuracy requirements for the FBI and their NCIC database.⁴⁷ EPIC warned that the exemption from keeping accurate records would result in significant risks to privacy, law enforcement and constitutional violations.⁴⁸ This campaign did not go unnoticed, and in 2004 numerous Congressmen and Senators introduced The Civil Liberties Restoration Act.⁴⁹ Title III of the bill required data entered into the NCIC database to meet the accuracy requirement of the Privacy Act.⁵⁰ Even with EPIC’s campaign and Congressional support, the bill died in the House Subcommittee on Crime, Terrorism and Homeland Security, and never became law.⁵¹ As if the quashing of this bill wasn’t enough, in December 2004, Congress passed the Intelligence Reform and Terrorism Prevention Act of 2004, which directed the president to “create an information sharing environment for the sharing of terrorism information in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties.”⁵²

An investigation conducted by the Government Accountability Office in 2005 found a myriad of errors in Department of Homeland Security databases.⁵³ The inaccuracies in government databases coupled with the lack of upkeep of their own advanced technology has caused the judiciary to react. In 2007, the federal district court in Northern California granted a temporary restraining order enjoining the Department of Homeland Security from implementing a verification program for employment eligibility.⁵⁴ The main reason the Court enjoined this program is because the numerous errors in Social Security Administration databases would result in unverified and inaccurate employment application reviews and deci-

sions.⁵⁵ However, while here a job applicant may have to wait months to obtain a job, the stakes are even higher during a criminal proceeding. Where government database accuracy plays a key role in law enforcement, it may mean the difference between liberty or a jail cell for the accused.

Herring v. United States

“What if an officer reasonably believes there is an outstanding arrest warrant, but that belief turns out to be wrong because of a negligent bookkeeping error by another police employee?”⁵⁶ On July 7, 2004, Bennie Herring went to the Coffee County Sheriff’s Department to retrieve something from his impounded truck.⁵⁷ Mark Anderson, an investigator for the Coffee County Sheriff’s Department asked the county warrant clerk, Sandy Pope, to check for any outstanding warrants for Herring’s arrest.⁵⁸ When the warrant search came back negative, Anderson asked the warrant clerk to investigate further and check with the neighboring Dale County.⁵⁹ After checking their computer database, the Dale County warrant clerk, Sharon Morgan, informed Anderson that there was an active arrest warrant for Herring’s failure to appear on a felony charge.⁶⁰ The warrant clerk from Dale County attempted to locate the hard-copy of the warrant to be faxed as confirmation.⁶¹

Anderson stopped Herring as he was leaving the impound lot, and a search incident to the arrest revealed methamphetamine in Herring’s pocket and a gun in his vehicle.⁶² However, there had been a mistake about the warrant:

The Dale County sheriff’s computer records are supposed to correspond to actual arrest warrants, which the office also maintains. But when Morgan went to the files to retrieve the actual warrant to fax to Pope, Morgan was unable to find it. She called a court clerk and learned that the warrant had been recalled five months earlier. Normally when a warrant is recalled the court clerk’s office or a judge’s chambers calls Morgan, who enters the information in the sheriff’s computer database and disposes of the physical copy. For whatever reason, the information about the recall of the warrant for Herring did not appear in the database. Morgan immediately called Pope to alert her to the mixup, and Pope contacted Anderson over a secure radio. This all unfolded in 10 to 15 minutes, but Herring had already been arrested and found with the gun and drugs, just a few hundred yards from the sheriff’s office.⁶³

Bennie Herring was indicted in the District Court for the Middle District Court of Alabama for illegally possessing the gun and drugs in violation of 18 U.S.C. § 922(g)(1)⁶⁴ and 21

U.S.C. § 844(a).⁶⁵ He moved to suppress the seized evidence on the ground that the initial search conducted incident to the arrest had been illegal because the warrant had been rescinded five weeks prior.⁶⁶ The Magistrate Judge recommended to deny the motion because the arresting officers had acted in a good-faith belief that the warrant was still outstanding and valid.⁶⁷ The Magistrate Judge reasoned that even if there were a Fourth Amendment violation, there was “no reason to believe that application of the exclusionary rule here would deter the occurrence of any future mistakes.”⁶⁸ The District Court adopted the Magistrate Judge’s recommendation, and Herring was convicted for illegally possessing the gun and drugs.⁶⁹

In affirming the District Court’s decision, the Eleventh Circuit Court of Appeals found that the arresting officers in Coffee County “were entirely innocent of any wrongdoing or carelessness.”⁷⁰ The Supreme Court further affirmed Herring’s conviction, following the reasoning set forth in *Evans*, reasoning that the mistake was made by a court clerk, and not by a police officer.⁷¹ However, the *Herring* Court further narrowed the exclusionary rule by setting an even higher burden for defendants to invoke the exclusionary rule on the basis of an error in a government database, specifically an outdated, invalid warrant:

To trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system. As laid out in our cases, the exclusionary rule serves to deter *deliberate, reckless, or grossly negligent conduct*, or in some circumstances recurring or systemic negligence.⁷²

Finally, the true effects of the *Herring* decision may lay in future cases with similar but a few distinguishing facts. According to the *Herring* Court, “we do not suggest that all recordkeeping errors by the police are immune from the exclusionary rule. In this case, however, the conduct at issue was not so objectively culpable as to require exclusion.”⁷³ However it seems that the Court is concerned with habitual problems, not just one-time occurrences. The numerous government database errors pointed out by Herring during oral arguments were dismissed by the Court because there was no evidence presented that errors in Dale County’s warrant system were routine or widespread.⁷⁴ However, with all the errors in the NCIC and other government databases, it is only a matter of time before the issue in *Herring* resurfaces and the Supreme Court, or a lower court, will again have to confront this issue. Until the Court changes its current position, individuals will continue to be convicted on evidence seized

in violation of the Fourth Amendment. Another shift in Fourth Amendment jurisprudence is needed to bring fairness back to the courtroom.

Analysis

Effect of the *Herring* Decision

There was a time that the exclusionary rule could be simply stated: “In *Weeks v. United States*,⁷⁵ this Court [the Supreme Court] held that in a federal prosecution the Fourth Amendment barred the use of evidence secured through an illegal search and seizure.”⁷⁶ But the Supreme Court’s holding in *Herring v. United States* represents a continuing shift in the narrowing application of the exclusionary rule.⁷⁷ The Supreme Court made what appears to be a fundamental shift in exclusionary rule analysis, by holding that a Fourth Amendment violation does not necessarily trigger the rule “if the underlying police error was merely negligent and not sufficiently deliberate that exclusion of evidence could meaningfully deter it.”⁷⁸ According to Steve Posner, “Herring represents a policy decision by the Court that convicting criminals is more important than preventing citizen victimization due to police negligence in record keeping, unless such errors are shown to be so widespread or systematic that police would be reckless in relying on the particular database at issue.”⁷⁹ While it is true that the holding of *Herring* can be read broadly or narrowly, the true effect will be seen in future suppression disputes in trial courts that try to interpret and apply the decision. A broad reading by lower courts could mean “the death of the exclusionary rule as a practical matter.”⁸⁰ Accordingly, the recent decision in *Herring* has already sparked controversy amongst commentators, journalists, and courts with some declaring the decision a landmark case and others dismissing the case as a blip on the constitutional radar.⁸¹ In fact, on the day *Herring* was decided, Tom Goldstein, a Washington lawyer who has argued numerous cases before the Supreme Court, blogged, “My preliminary reaction is that we will at some point soon regard today’s *Herring* decision as one of the most important [Fourth Amendment] rulings... in the last quarter century.”⁸²

However, what scholars are missing in debating whether the *Herring* holding is broad or narrow is that the facts of *Herring* are likely to happen again. The situation is significantly more likely to happen than most people think based on the numerous errors in government databases.⁸³ As technology evolves, law enforcement officials are increasingly using a vast, cross-referencing system of public and private databases, both of which contain numerous errors.⁸⁴ In these

inter-linked databases, one error can spread like a disease, infecting every system it touches, plaguing the individual with false records and undue suspicion.⁸⁵

The EPIC amicus curiae brief in the *Herring* case highlights the numerous errors present in government databases, and how the factual situation in *Herring* will likely repeat itself. According to the Bureau of Justice Statistics (“BJS”), “in the view of most experts, inadequacies in the accuracy and completeness of criminal history records is *the single most serious deficiency* affecting the Nation’s criminal history record systems.”⁸⁶ Years later, the problem persists. In a 2005 report, the BJS detailed ongoing concerns about errors in the NCIC database and targets the problem to state criminal history records which are then fed into the NCIC.⁸⁷ According to the 2005 report, “surveys have suggested that criminal history repositories are encountering several problems including significant backlogs, older records that have no dispositions, and infrequent audits to ensure accuracy of records.”⁸⁸ For example, a man faced a similar predicament as Bennie Herring when a computer report listed him as committing “numerous crimes he never committed.”⁸⁹ Specifically the computer report listed him as a female prostitute in Florida, an inmate currently incarcerated in Texas for manslaughter, a stolen goods dealer in New Mexico, a witness tamperer in Oregon, and a registered sex offender in Nevada.⁹⁰ Record accuracy was an issue long before Bennie Herring was searched pursuant to an invalid warrant, and it will continue to be a problem the lower courts must deal with while applying *Herring*.

Arguably, with *Herring* comes a shift from requiring suppression of physical evidence due to police misconduct to “other ways to deter police wrongdoing directly, including professional discipline, civil lawsuits and criminal prosecution.”⁹¹ The Court generally established that an officer’s negligent error does not trigger the exclusionary rule: “As laid out in our cases, the exclusionary rule serves to deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence.”⁹² Yet, it is hard to ignore the fact that in refusing to exclude the evidence gained from Herring’s illegal arrest and search, the Court diminished everyone’s right against unreasonable searches and seizures.⁹³ *Herring* actually undermines the Supreme Court decisions that came before emphasizing the importance of the exclusionary rule.⁹⁴ The *Mapp* Court regarded the exclusionary rule as so critical that it surmised that failure to use it would reduce the right against unreasonable search and seizure to “a form of words, valueless and undeserving of mention in a perpetual charter of inestimable human liberties.”⁹⁵ By forbidding use of the Fourth Amendment’s most

effective remedy, the exclusionary rule, to deter law enforcement’s careless computer errors, the *Herring* Court signaled to police that negligent maintenance of records will have no practical consequences in the courtroom.⁹⁶ A Fourth Amendment violation, an illegal search and seizure based on false or mistaken computer records, now passes constitutional muster and the evidence will not be suppressed.

Justice Ruth Bader Ginsburg warned of this type of incident in the *Evans* case: “The offense to the dignity of the citizen who is arrested, handcuffed, and searched on a public street simply because some bureaucrat has failed to maintain an accurate computer data base strikes me as equally outrageous.”⁹⁷ Additionally, Justice Ginsburg predicted how the errors and mistakes in government databases would cause more problems in the future:

[W]idespread reliance on computers to store and convey information generates, along with manifold benefits, new possibilities of error, due to both computer malfunctions and operator mistakes. Most germane to this case, computerization greatly amplifies an error’s effect, and correspondingly intensifies the need for prompt correction; for inaccurate data can infect not only one agency, but the many agencies that share access to the data base.⁹⁸

In addition to *Herring*, the *Evans* decision provides no protection to those who fall victim to police and computer database error. *Evans*, as discussed above, involved a police search of defendant’s car pursuant to an outstanding warrant.⁹⁹ However, despite the warrant being in the Sheriff’s Office’s database, the warrant had been quashed seventeen days prior to the arrest.¹⁰⁰ In refusing to apply the exclusionary rule, the *Evans* Court concluded that “exclusion of evidence at trial would not sufficiently deter future errors [by court employees] so as to warrant such a severe sanction.”¹⁰¹ While the Supreme Court in both *Evans* and *Herring* pointed out that no evidence existed to support the proposition “that court employees [were] inclined to ignore or subvert the Fourth Amendment,”¹⁰² they ignored the proposition that without the exclusionary rule or any further penalties, clerks and employees have no reason or incentive to keep accurate, updated records.

The standard set in *Herring* makes it almost impossible for defendants to get a fair trial and obtain an appropriate remedy for violations of their Fourth Amendment rights. Only, for example, where “police have been shown to be reckless in maintaining a warrant system, or to have knowingly made false entries to lay the groundwork for future false arrests” will the exclusionary rule be applied.¹⁰³ As an attorney with

criminal defense experience, I am troubled by this standard since these new barriers for invoking the exclusionary rule in cases involving database errors seem insurmountable. How are defendants supposed to gain insight and knowledge into warrant and other government database management? And as a practical matter, how is a defendant going to prove at an evidentiary hearing, with evidence and testimony, that the clerks or employees recklessly maintained or made false entries in the system? Steve Posner attempted to answer these questions and practical concerns facing criminal defendants:

After *Herring*, the practitioner who seeks to suppress evidence based on a police record-keeping error, or any issue involving a law enforcement database, should consider whether to subpoena or otherwise discover the entire police file and review it for evidence of record-keeping errors, in order to prove that police who rely on that database are reckless. As a practical matter, and as recognized by the *Herring* dissent, this is an expensive proposition that impoverished defendants may not be able to afford, and when a defendant can afford it, production and audit of police databases will be burdensome on police and the courts, and will be opposed on that basis.¹⁰⁴

Without answers to these questions, criminal defendants will face a drastic reduction in their Fourth Amendment rights, resulting in an unfair trial with, what has historically been deemed, inadmissible evidence.

Herring in Practice

The Johnson case out of Louisiana state court is a prime example of how *Herring* affected one defendant negatively and actually shifted the tides mid-litigation.¹⁰⁵ Shortly before *Herring* was decided, Robert Johnson was involved in a similar situation as Bennie Herring:

Robert Johnson was initially stopped by an NOPD [New Orleans Police Department] officer after the officer observed Johnson driving without a seat belt. Upon running Johnson's name through NOPD's CAD [Computer Aided Dispatch] system and finding an outstanding warrant on Johnson, the officer arrested him, and searched him incidental to the arrest. The search revealed a small amount of marijuana in Johnson's pocket. Before leaving the scene, the officer attempted to run Johnson's name through the NCIC system to verify the validity of the warrant; the NCIC system was down. The officer proceeded to central lockup. Once there, the officer requested deputies to check the warrant again. The warrant was no longer valid. However,

Johnson was booked and charged with one count of first offense possession of marijuana...¹⁰⁶

The defendant moved to suppress the marijuana arguing that the officer should have attempted to run Johnson's name through NCIC to verify the validity of the warrant before conducting a search incident to arrest.¹⁰⁷ The trial court agreed with the defense and, in suppressing the evidence, held that the officer "could have waited on scene for some undetermined amount of time before Johnson was arrested and searched."¹⁰⁸ As of this point, prior to the *Herring* decision, the evidence was suppressed and the defendant experienced significantly lesser consequences due to an error in a state warrant database.¹⁰⁹ However, immediately after the *Herring* decision, the State appealed the trial court in light of the *Herring* Court's new views on defective warrants in governmental databases and how the exclusionary rule should be applied.¹¹⁰

As the Court of Appeal of Louisiana for the Fourth Circuit stated, "the United States Supreme Court cleared up this previously murky area of law."¹¹¹ The Appeals Court reversed the trial court's ruling, and held that "the officer in this case acted in good faith when he arrested Johnson based on the information available to him at the time."¹¹² The defendant had won his motion in trial court; the case seemingly was over for the prosecution.¹¹³ Yet, within weeks of the *Herring* decision, this appeal was granted, the trial court's ruling was reversed, and the prosecution was now allowed to use evidence that was obtained through a search predicated on an invalid warrant in an un-updated warrant management system. There are also other cases where the prosecution has attempted to turn the tide on defendants with the *Herring* decision.

On March 12, 2007, agents of Immigration and Customs Enforcement ("ICE") submitted an application and affidavit in support of a warrant to search John Perry Ryan's house.¹¹⁴ The warrant was granted; however, although the items to be seized were described in the application and affidavit, the warrant contained no such description.¹¹⁵ Upon executing the search warrant, federal agents seized computers, a wireless media card, documents and photographs.¹¹⁶ These items did appear in a list attached to the application for a search warrant, but were not attached to the actual search warrant.¹¹⁷ A grand jury indicted Ryan for transporting and possessing child pornography based on what was recovered and contained on the seized electronics.¹¹⁸

The defense moved to suppress the evidence seized based on the defective search warrant, and the court granted the motion to suppress on March 31, 2008.¹¹⁹ However, in light of *Herring*, the government moved the Court in February

2009 to reconsider its March 31, 2008 ruling under Federal Rule of Civil Procedure 60(b).¹²⁰ According to the Vermont District Court, *Herring* addresses the issue of whether the good faith exception to the exclusionary rule applies when the police make a negligent error in the execution of a warrant.¹²¹ The government in this case likened the clerk and officer's failure to attach the list of items to be seized to the search warrant to the negligent warrant database maintenance in *Herring*. However, in reconsidering its prior decision, the District Court affirmed the suppression of the illegally seized evidence, distinguishing this case from *Herring*: "This is a critical distinction from *Herring*. The law enforcement officers in *Herring* relied upon apparently reliable information that existed. In this case, the agents relied upon a facially invalid warrant that failed to particularly describe the items to be seized. Exclusion is appropriate where a 'warrant was so lacking in the indicia of probable cause that an objectively reasonable officer should not have relied on it.'"¹²²¹²³

There is also little doubt that technology played a commanding role in the *Herring* decision as evidenced by the concerns and comments made by the Justices during oral arguments. As Chief Justice Roberts commented during oral arguments of the case, police have limited resources in the area of police recordkeeping and "probably don't have the latest version of WordPerfect, or whatever it is."¹²⁴ However, as the *Robinson* case out of the Supreme Court of California shows, even police officers with the most advanced technology make mistakes that lead to unreasonable searches, seizures and invasions upon an individual's privacy.¹²⁵ In this case, Paul Eugene Robinson was accused of committing five felony sexual offenses upon a Deborah L. in August of 1994.¹²⁶ In August of 2000, four days before the statute of limitations to bring criminal prosecution would have expired (6 years in California), the Sacramento County District Attorney filed a felony complaint against "John Doe, unknown male" describing him by his unique 13-loci deoxyribonucleic acid ("DNA") profile.¹²⁷ The next day, a John Doe arrest warrant was issued, incorporating by reference the same DNA profile, and Robinson was arrested in September of 2000.¹²⁸ However, the defendant's DNA profile in the state's DNA database, which linked Robinson to the crimes committed against Deborah L., had been generated from blood mistakenly collected from the defendant by local and state agencies in administering the DNA and Forensic Identification Database and Data Bank Act of 1998 ("the Act").¹²⁹ The Act was enacted while the defendant was incarcerated, serving a sentence for felony first degree burglary.¹³⁰ However, an unknown prison employee completed a DNA testing form in which the defendant was mistakenly identified as a prisoner

with a qualifying offense; as a result, a sample of the defendant's blood was drawn in violation of the Act.¹³¹ In fact, the parties both agreed that the defendant's earlier blood sample was collected in violation of the Act.¹³² The defense moved to suppress the DNA evidence at trial on the basis that the federal exclusionary rule was the appropriate "remedy to apply to the police personnel errors that occurred in this case."¹³³

Ultimately the California Supreme Court held that there was no violation of the Robinson's Fourth Amendment because as an incarcerated, convicted criminal, he did not have a valid privacy interest.¹³⁴ However, the *Robinson* Court then conducted an in-depth analysis of *Herring* and how it would apply if the court had found a Fourth Amendment violation.¹³⁵ The defense contended that the mistaken collection of his blood sample was the result of "a cascading series of errors" that "were indicative of a system breakdown."¹³⁶ The *Robinson* Court rejected this argument, and upheld the trial court's finding of fact that the mistakes that lead to the unlawful collection of the defendant's blood were made because "correctional staff was under pressure to immediately implement a newly enacted law that was complex and confusing," and the motivation for collecting the blood sample "was a good faith believe, possibly based on a negligent analysis by someone, that the defendant was a qualified offender."¹³⁷ Based on *Herring* and *Robinson*, it follows that local police departments in California will be given significant lee-way in conducting mistakes, and the result will be illegally seized evidence being admissible against defendants at trial.

Conclusion

Herring and technology have both contributed to sweeping changes in Fourth Amendment jurisprudence, specifically the exclusionary rule. In the modern age, where law enforcement is dependent on computers, the accuracy of government databases may determine whether a defendant gets a fair trial. Technology has played a major role in the area of Fourth Amendment search and seizure law through its use in law enforcement and the determination of probable cause. When probable cause for an arrest is founded on errors in government databases, the Supreme Court has allowed evidence obtained from that search into trial. As a result, individuals are having their Fourth Amendment rights violated during the illegal seizure, and when that evidence is introduced at trial.

Maintaining accurate record systems is one of the central requirements of information management. Moreover, the technology of government databases has changed dramatically since 1995, when the Court upheld the use of evidence

obtained from an erroneous arrest record that was the product of a clerical mistake. Today, the police have within their electronic reach access to an extraordinary range of databases. Mixed and mingled together are government and commercial databases filled with errors. Modern policing is a coordinated enterprise and it is critical that a commitment to accuracy is maintained throughout the criminal justice system. Not only does erroneous data affect the rights of citizens, it also undermines effective investigations by creating confusion and mistakes. What *Herring* has done is shed light on the sheer volume of errors that exist in government databases. However, what *Herring* has also done is leave criminal defendants vulnerable to these errors. *Herring* not only provides no protection to victims of government database errors or police negligent bookkeeping, it actually strips away a fundamental judicial remedy historically used to protect these victims. Short of a massive fishing expedition into an entire governmental database, which is impractical, defendants will have much more difficulty in suppressing evidence obtained through illegal searches and seizures. The result is unfair: the accused is faced with illegally seized evidence and local police departments receive no penalty for keeping incorrect records. As policing becomes more reliant on computerized systems, the number of illegal arrests and searches based on errors in government record-keeping is poised to multiply. And under *Herring*, the exclusionary rule is no longer a weapon in the defense's arsenal to combat these errors. ■

Endnotes

- 1 J.D. Suffolk University Law School, May 2010.
- 2 Milton Meltzer, *The Bill of Rights: How We Got It and What It Means* 5-6 (Thomas Crowell Publishers, 1990). The Bill of Rights were introduced by James Madison to the First United States Congress in 1789 and came into effect December 5, 1791 when they were ratified by three-fourths of the States. *Id.*
- 3 *Olmstead v. United States*, 277 U.S. 438, 457-57 (1928) (Brandeis, J., dissenting).
- 4 Robert L. Farb, *The Fourth Amendment, Privacy, and Law Enforcement*, POPULAR GOVERNMENT, May 17, 2009, at 13-19, available at <http://www.sog.unc.edu/pubs/electronicversions/pg/pgspr02/article2.pdf>.
- 5 See *United States v. Leon*, 468 U.S. 897, 909 (1984) (carving out good-faith exception to the exclusionary rule).
- 6 U.S. CONST. AMEND. IV. The Fourth Amendment States: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." *Id.*
- 7 *Weeks v. United States*, 232 U.S. 383, 393 (1914). A unanimous Court determined that in order for the Fourth Amendment to have bite and redress for violations, evidence obtained by way of illegal searches and seizures must be excluded from use in federal criminal prosecutions. *Id.*
- 8 *Id.* at 398.
- 9 *Id.* at 394.
- 10 *Weeks*, 232 U.S. at 398. "The Fourth Amendment is not directed to individual misconduct of such [state] officials. Its limitations reach the Federal Government and its agencies." *Id.*
- 11 Bernard Schwartz, *Commentary, Chief Justice Warren and 1984*, 35 HASTINGS L.J. 975, 979-80 (1984).
- 12 See *Mapp v. Ohio*, 367 U.S. 643 (1961) (Incorporating the Exclusionary Rule to apply to state criminal prosecutions through the Fourteenth Amendment); see also *Katz v. U.S.*, 389 U.S. 347 (1967) (overturning a state conviction for illegal gambling based on a Fourth Amendment violation).
- 13 *Mapp*, 367 U.S. at 643.
- 14 *Id.*
- 15 *Mapp*, 367 U.S. at 657. Justice Clark stated "our holding that the exclusionary rule is an essential part of both the Fourth and Fourteenth Amendments is not only the logical dictate of prior cases, but it also makes very good sense. There is no war between the Constitution and common sense." *Id.*
- 16 *United States v. Leon*, 468 U.S. 897, 909 (1984) (holding that evidence obtained in good faith by police relying upon a search warrant that is subsequently invalidated may be used in criminal trial).
- 17 *Id.* at 900-2.
- 18 *Id.* at 908.
- 19 *Leon*, 468 U.S. at 918. "If the purpose of the exclusionary rule is to deter unlawful police conduct, then evidence obtained from a search should be suppressed only if it can be said that the law enforcement officer had knowledge, or may properly be charged with knowledge, that the search was unconstitutional under [the Fourth Amendment]." *Id.* at 919.
- 20 Benjamin J. Robinson, *Comment, CONSTITUTIONAL LAW: SUPPRESSING THE EXCLUSIONARY RULE*, 59 FLA. L. REV. 475, 479 (2007); see *Arizona v. Evans*, 514 U.S. 1 (1995).
- 21 See Robinson, *supra* note 20, at 479.
- 22 See Robinson, *supra* note 20, at 479.
- 23 *Arizona v. Evans*, 514 U.S. at 4. "At the suppression hearing, the Chief Clerk of the Justice Court testified that a Justice of the Peace had issued the arrest warrant on December 13, 1990, because respondent had failed to appear to answer for several traffic violations. On December 19, 1990, respondent appeared before a *pro tem* Justice of the Peace who entered a notation in respondent's file to "quash warrant." *Id.* at 4-5.
- 24 *Evans*, 514 U.S. at 5.
- 25 *Id.* at 6.
- 26 *Id.* at 11.
- 27 *Evans*, 514 U.S. at 15.

- 28 Shawn B. Spencer, *SECURITY VS. PRIVACY: reframing the debate*, 79 DENV. U. L. REV. 519, 521 (2002); see also FBI website discussing NCIC, available at <http://www.fas.org/irp/agency/doj/fbi/is/ncic.htm>.
- 29 Spencer, *supra* note 27.
- 30 *Id.*
- 31 See Department of Homeland Security Privacy Impact Assessment at n.2 (2003), available at http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0333.xml.
- 32 See 28 U.S.C. § 534 (2009) (authorizing Attorney General to delegate to the Director of the FBI the duty of acquiring, preserving and exchanging criminal and identification records and information) (*amended* 1988, Uniform Federal Crime Reporting Act of 1988).
- 33 Privacy Act, 5 U.S.C. §552 (2009). The statute defines agencies covered under the Act as “any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency.” *Id.*
- 34 *Id.*
- 35 Menard v. Saxbe, 498 F.2d 1017, 1026 (1974) (requiring the FBI to expunge NCIC record where individual was only detained and not formally arrested).
- 36 *Id.* at 1026.
- 37 John Shattuck – Biography, available at <http://www.jfklibrary.org/JFK+Library+and+Museum/Kennedy+Library+Foundation /Administration+and+Staff/John+Shattuck+Bio.htm>.
- 38 John Shattuck, *In the Shadow of 1984: National Identification Systems, Computer-Matching, and Privacy in the United States*, 35 HASTINGS L.J. 991, 994 (1984).
- 39 *Id.*
- 40 *Id.*
- 41 See Congressional Response Report by The Office of the Inspector General of the Social Security Administration, *Accuracy of the Social Security Administration’s Numident File*, Report A-08-06-26100 (2006), available at <http://www.ssa.gov/oig/ADOBEPDF/A-08-06-26100.pdf>. The report found numerous accuracy problems in databases of citizenship, immigration statistics and Social Security Administration databases. *Id.* The Inspector General estimated and confirmed that about 18 million records in the Social Security Administration files have discrepancies with name, date of birth or death, and citizenship status. *Id.*
- 42 See Department of Justice Office of the Inspector General Report, *Immigration and Naturalization Service Monitoring of Nonimmigrant Overstays*, Report I-97-08 (1997), available at <http://www.usdoj.gov/oig/reports/INS/e0304/results.htm>.
- 43 See Department of Homeland Security Proposed Rule, *Privacy Act of 1974: Implementation of Exemptions; Automated Targeting System*, Docket Number: 2007-0043 (Dept. of Homeland Security receiving an exemption from requiring accuracy of its terrorist risk assessment database), available at http://www.dhs.gov/xnews/releases/pr_1186178812301.shtm.
- 44 *Id.*
- 45 *Id.*
- 46 Exemption of Federal Bureau of Investigation, 28 C.F.R. 16.96 (2009). This regulation also exempted the Central Records System and National Center for the Analysis of Violent Crime systems from accuracy requirements of the Privacy Act. *Id.*
- 47 See EPIC’s Interest in the Herring Case, available at <http://epic.org/privacy/herring/#err>.
- 48 *Id.*
- 49 Civil Liberties Restoration Act of 2004, H.R.4591, 109th Cong. (2004). Among the many prominent Congressmen are Representative Howard Berman (CA) and Representative William Delahunt (MA). Additionally, Senators Edward Kennedy (MA), Senator Richard Durbin (IL), Senator Russ Feingold (WI), and Senator Jon Corzine (NJ) introduced the Senate counterpart of the Civil Liberties Restoration Act, S 2528, 109th Cong. (2004). *Id.*
- 50 David Carney, *Legislators Introduce Bills Pertaining to NCIC Database*, TECH LAW JOURNAL, NEWS from June 16-20, 2004, available at <http://www.techlawjournal.com/home/newsbriefs/2004/06d.asp>. In proposing the bill to the Senate, Senator Edward Kennedy of Massachusetts stated “Our bill protects the integrity of the National Crime Information Center database. For decades, in maintaining the database, the Department of Justice was required to obey the Privacy Act, which requires each agency to maintain its records with such accuracy, relevance, timeliness and completeness as is reasonably necessary to assure fairness to the individuals determination.” *Id.*
- 51 H.R. 4591, 109th Cong. (2004), GOVTRACK.US, May 17, 2009, available at <http://www.govtrack.us/congress/bill.xpd?bill=h108-4591>.
- 52 Brief of Amici Curiae Electronic Privacy Information Center (EPIC), *et al.* in Support of Petitioner, Herring v. United States, 2007 U.S. Briefs 513, 11-12 (2009); see Pub. L. No. 108-458, 118 Stat. 3638 (2004).
- 53 United States Accountability Office Report to Congressional Requesters, *Immigration Enforcement: Weaknesses Hinder Employment Verification and Worksite Enforcement Efforts*, Report GAO-05-813 (2005), available at <http://www.gao.gov/new.items/d05813.pdf>.
- 54 Am. Fed’n of Labor v. Chertoff, Order Granting Motion for Preliminary Injunction, No. C 07-04472 CRB (October 10, 2007), available at http://www.aclu.org/images/asset_upload_file505_32133.pdf.
- 55 *Id.* at 7. Under the proposed program for employment application verification, any disputed social security numbers would be sent to the Social Security Administration (“SSA”) for verification. *Id.* It would usually take 90 days for a response, and any letter that indicated there was no match in the SSA database would restart the entire process. *Id.* The flaw in this program is that the numerous inaccuracies in the SSA databases would result in No-Match letters would prevent eligible applicants from obtaining employment. *Id.* Through no fault of their own, qualified applicants would be denied work, and the SSA was making little effort to upgrade their technology or improve the accuracy of their databases. *Id.* at 9.

- 56 *Herring v. United States*, 129 S. Ct. 695, 698 (2009) (Roberts, J.).
- 57 *Herring*, 129 S.Ct. at 698.
- 58 *Id.*
- 59 *Id.*
- 60 *Id.*
- 61 *Herring*, 129 S. Ct. at 698.
- 62 *Id.*; see 18 U.S.C. §992(g)(1) (2009) (prohibiting a felon to be in possession of a firearm).
- 63 *Herring*, 129 S. Ct. at 698.
- 64 18 U.S.C. §922(g)(1) states: It shall be unlawful for any person who has been convicted in any court of, a crime punishable by imprisonment for a term exceeding one year...to ship or transport in interstate or foreign commerce, or possess in or affecting commerce, any firearm or ammunition; or to receive any firearm or ammunition which has been shipped or transported in interstate or foreign commerce.
- 65 21 U.S.C. § 844(a) states: (a) Unlawful acts; penalties. It shall be unlawful for any person knowingly or intentionally to possess a controlled substance unless such substance was obtained directly, or pursuant to a valid prescription or order, from a practitioner, while acting in the course of his professional practice, or except as otherwise authorized by this title or title III. It shall be unlawful for any person knowingly or intentionally to possess any list I chemical obtained pursuant to or under authority of a registration issued to that person under section 303 of this title [21 USCS § 823] or section 1008 of title III [21 USCS § 958] if that registration has been revoked or suspended, if that registration has expired, or if the registrant has ceased to do business in the manner contemplated by his registration. It shall be unlawful for any person to knowingly or intentionally purchase at retail during a 30 day period more than 9 grams of ephedrine base, pseudoephedrine base, or phenylpropanolamine base in a scheduled listed chemical product, except that, of such 9 grams, not more than 7.5 grams may be imported by means of shipping through any private or commercial carrier or the Postal Service. Any person who violates this subsection may be sentenced to a term of imprisonment of not more than 1 year, and shall be fined a minimum of \$ 1,000, or both, except that if he commits such offense after a prior conviction under this title or title III, or a prior conviction for any drug, narcotic, or chemical offense chargeable under the law of any State, has become final, he shall be sentenced to a term of imprisonment for not less than 15 days but not more than 2 years, and shall be fined a minimum of \$ 2,500, except, further, that if he commits such offense after two or more prior convictions under this title or title III, or two or more prior convictions for any drug, narcotic, or chemical offense chargeable under the law of any State, or a combination of two or more such offenses have become final, he shall be sentenced to a term of imprisonment for not less than 90 days but not more than 3 years, and shall be fined a minimum of \$ 5,000. Notwithstanding the preceding sentence, a person convicted under this subsection for the possession of a mixture or substance which contains cocaine base shall be imprisoned not less than 5 years and not more than 20 years, and fined a minimum of \$ 1,000, if the conviction is a first conviction under this subsection and the amount of the mixture or substance exceeds 5 grams, if the conviction is after a prior conviction for the possession of such a mixture or substance under this subsection becomes final and the amount of the mixture or substance exceeds 3 grams, or if the conviction is after 2 or more prior convictions for the possession of such a mixture or substance under this subsection become final and the amount of the mixture or substance exceeds 1 gram. Notwithstanding any penalty provided in this subsection, any person convicted under this subsection for the possession of flunitrazepam shall be imprisoned for not more than 3 years, shall be fined as otherwise provided in this section, or both. The imposition or execution of a minimum sentence required to be imposed under this subsection shall not be suspended or deferred. Further, upon conviction, a person who violates this subsection shall be fined the reasonable costs of the investigation and prosecution of the offense, including the costs of prosecution of an offense as defined in sections 1918 and 1920 of title 28, United States Code, except that this sentence shall not apply and a fine under this section need not be imposed if the court determines under the provision of title 18 that the defendant lacks the ability to pay.
- 66 *Herring*, 129 S.Ct. at 699.
- 67 *Id.*; see *U.S. v. Herring*, 451 F. Supp. 2d 1290 (October 26, 2005) (District Court Judge's order adopting the Magistrate Judge's recommendation and discussing the reasoning by the Magistrate Judge).
- 68 *Herring*, 129 S. Ct. 695, 699; see 451 F. Supp. 2d 1290.
- 69 *Herring*, 129 S.Ct. at 699; see 451 F. Supp. 2d 1290 (District Court Judge's order adopting the Magistrate Judge's recommendation to deny Herring's motion to suppress).
- 70 *U.S. v. Herring*, 492 F.3d 1212, 1218 (11th Cir. 2007) (holding that even though the defendant's Fourth Amendment rights were violated, suppression was not required because while the county's failure to update its records may have been negligent, applying the exclusionary rule would not deter bad record keeping in the future).
- 71 129 S.Ct. at 701.
- 72 *Herring*, 129 S. Ct. at 702 (emphasis added).
- 73 *Id.* at 703.
- 74 *Id.* at 704.
- 75 *Weeks v. United States*, 232 U.S. 383 (1914) (holding that evidence obtained in violation of the Fourth Amendment's prohibition against unreasonable searches and seizures must be excluded from use in federal criminal prosecutions).
- 76 Steve C. Posner, *Herring v. United States, the Exclusionary Rule, and the USA PATRIOT Act "Fall of the Wall,"* 2009 Emerging Issues 3647, 1 (2009) (Lexis Nexis Emerging Issues Newsletter). Steve Posner is the author of the annually updated legal treatise *Privacy Law and the USA PATRIOT Act* (LexisNexis/Matthew Bender 2006), and Mr. Posner frequently speaks on privacy and national security law to professional and community groups, as well as undergraduate and graduate level university classes. *Id.* at 4. Mr. Posner is a former editor of the Technology Law and Policy Review column for *The Colorado Lawyer* magazine, and former co-chair of the Colorado Bar Association's Law and Technology Committee. *Id.* at 4.

- 77 Lieutenant Colonel Stephen R. Steward, “Damn the Torpedoes” – Fourth Amendment Search and Seizure Law in the 2008 Military Appellate Term of Court, 2009 *ARMY LAW* 19, 34 (2009). Lt. Cl. Steward is a Professor in the Criminal Law Department at The Judge Advocate General’s Legal Center and School, U.S. Army, in Charlottesville, Virginia. *Id.*
- 78 See Posner, *supra* note 76, at 1.
- 79 See Posner, *supra* note 76, at 1-2.
- 80 *Id.* at 34.
- 81 Matthew Allan Josephson, *To EXCLUDE OR NOT TO EXCLUDE: THE FUTURE OF THE EXCLUSIONARY RULE AFTER HERRING V. UNITED STATES*, 42 *CREIGHTON L. REV.* 175, 176-77 (2009).
- 82 Albert W. Alschuler, *Herring v. United States: A Minnow or a Shark?*, 7 *OHIO ST. J. CRIM. L.* 463, 472 (Fall 2009); see Tom Goldstein, *The Surpassing Significance of Herring*, SCOTUSBlog, January 14, 2009, available at <http://www.scotusblog.com/2009/01/the-surpassing-significance-of-herring/>.
- 83 See Department of Justice Office of the Inspector General Report, *Immigration and Naturalization Service Monitoring of Nonimmigrant Overstays*, Report I-97-08 (1997). available at <http://www.usdoj.gov/oig/reports/INS/e0304/results.htm>.
- 84 Brief of Amici Curiae Electronic Privacy Information Center (EPIC), *et al.* in Support of Petitioner, *Herring v. United States*, 2007 U.S. Briefs 513, 7 (2009).
- 85 *Id.*
- 86 Brief of Amici Curiae Electronic Privacy Information Center (EPIC), *et al.* in Support of Petitioner, *Herring v. United States*, 2007 U.S. Briefs, 513, 14,(2007) (emphasis in the original); see Bureau of Justice Statistics, *Use and Management of Criminal History Record Information: A Comprehensive Report*, 2001 Update, NCJ 187670 at 38 (Dec. 2001).
- 87 See Bureau of Justice Statistics, *Improving Access to and Integrity of Criminal History Records*, NCJ 200581 (July 2005) (detailing errors in the NCIC database and its relation to state criminal databases).
- 88 *Id.* at 11 (discussing that state repositories must make significant changes in order to improve the NCIS background check process).
- 89 George M. Dery, III, *Good Enough for Government Work: The Court’s Dangerous Decision, In Herring v. United States, to Limit the Exclusionary Rule to Only the Most Culpable Police Behavior*, 20 *GEO. MASON U. CIV. RTS. L.J.* 1, 2 (Fall 2009).
- 90 *Id.* at 2; see Brief of Amici Curiae Electronic Privacy Information Center (EPIC), Privacy and Civil Rights Organizations, and Legal Scholars and Technical Experts in Support of Petitioner at 18-19, *Herring v. United States*, 129 S. Ct. 695 (2009) (No. 07-513), 2008 WL 2095709.
- 91 Adam Liptak, *Justices Step Closer to Repeal of Evidence Ruling*, *N.Y. TIMES*, Jan. 31, 2009, at A1, available at <http://www.nytimes.com/2009/01/31/washington/31scotus.html>.
- 92 *Herring*, 129 S. Ct. at 702.
- 93 See DOJ Report, *supra* note 83, at 34.
- 94 See DOJ Report, *supra* note 83, at 34.
- 95 *Mapp v. Ohio*, 367 U.S. 643, 655 (1961).
- 96 See Posner, *supra* note 83, at 34.
- 97 *Arizona v. Evans*, 514 U.S. 1, 23 (1995) (Ginsburg & Stevens, JJ. dissenting).
- 98 *Id.* at 26 (Ginsburg, & Stevens, JJ., dissenting).
- 99 *Evans*, 514 U.S. 1 (1995).
- 100 *Id.* at 4.
- 101 Sean D. Doherty, *The End Of An Era: Closing The Exclusionary Debate Under Herring V. United States*, 37 *HOFSTRA L. REV.* 839, 858 (Spring 2009).
- 102 *Arizona v. Evans*, 514 U.S. at 14-15 (1995).
- 103 See Doherty, *supra* note 101, at 860.
- 104 See Posner, *supra* note 76, at 3.
- 105 See *State of Louisiana v. Johnson*, 6 So. 3d 195 (2005) (reversing the court’s earlier ruling to suppress evidence in light of the *Herring* decision).
- 106 *Johnson*, 6 So. 3d. at 196.
- 107 *Id.*
- 108 *Id.*
- 109 See *Johnson*, 6 So. 3d 195 (discussing the trial court suppressing the evidence due to the error in the warrant database).
- 110 *Id.*; see *United States Herring*, 129 S. Ct. 695.
- 111 *Johnson*, 6 So. 3d 195, 196 (referring to the *Herring* decision being dispositive on issue in this case).
- 112 *Id.*
- 113 *Id.*
- 114 *United States v. Ryan*, 2008 U.S. Dist. LEXIS 29690, 2 (March 31, 2008).
- 115 *Id.*
- 116 *Id.* at 3.
- 117 *Id.*
- 118 In violation of 18 U.S.C. §§2252A(a)(1) & 2252A(a)(5)(B); see *Ryan*, 2008 U.S. Dist. LEXIS 29690 at 3.
- 119 *United States v. Ryan*, 2009 U.S. LEXIS 53644, 3-4 (May 26, 2009).
- 120 *Id.* at 2-4; see Fed. R. Civ. P. 60(b), which states: Grounds for Relief from a Final Judgment, Order, or Proceeding. On motion and just terms, the court may relieve a party or its legal representative from a final judgment, order, or proceeding for the following reasons:
- (1) mistake, inadvertence, surprise, or excusable neglect;
 - (2) newly discovered evidence that, with reasonable diligence, could not have been discovered in time to move for a new trial under Rule 59(b);
 - (3) fraud (whether previously called intrinsic or extrinsic), misrepresentation, or misconduct by an opposing party;
 - (4) the judgment is void;
 - (5) the judgment has been satisfied, released, or discharged; it is based on an earlier judgment that has been reversed or vacated; or applying it prospectively is no longer equitable; or
 - (6) any other reason that justifies relief.

- 121 *Ryan*, 2009 U.S. LEXIS 53644 at 4.
- 122 *United States v. Lindsey*, 596 F. Supp. 2d 55, 62 (D. D. C. 2009) (finding, *post-Herring*, that the good faith exception in *Leon* did not apply where “an objectively reasonable officer could not have relied on the warrant in this case” and suppressing evidence found in search of home where search warrant was based on stale evidence) (citation omitted).
- 123 *United States v. Lester*, 2009 U.S. Dist. LEXIS 29631, 2009 WL 902354, at *6-7 (W. D. Va. Apr. 1, 2009) (distinguishing *Herring* and finding that officers could not reasonably rely on search warrant because it was not based on probable cause) (citation omitted).
- 124 Transcript of Oral Argument at 20, *Herring*, 129 S.Ct. 695 (No. 07-513), available at http://www.supremecourtus.gov/oral_arguments/argument_transcripts/07-513.pdf.
- 125 See *People v. Robinson*, 47 Cal. 4th 1104 (January 2010) (holding that the exclusionary rule was not triggered where the police were negligent in implementing a new Act requiring a new DNA database that resulted in an unwarranted blood sample to be taken from the defendant).
- 126 *Robinson*, 47 Cal 4th at 1111.
- 127 *Robinson*, 47 Cal 4th 1104, 1112-13; see California Penal Code §§ 959, par 4, 815, permitting the use of fictitious names in charging documents; see also *People v. Montoya*, 255 Cal. App. 2d 137(1967) (holding that if a fictitious name is used the warrant should also contain sufficient descriptive material to indicate with reasonable particularity the identification of the person whose arrest is ordered).
- 128 *Robinson*, 47 Cal 4th at 1113.
- 129 *Id.*; see California Penal Code §295 (creating a state-wide DNA database and requiring DNA samples from “all persons, including juveniles, for the felony and misdemeanor offenses described...”).
- 130 *Robinson*, 47 Cal 4th at 1118.
- 131 *Id.*
- 132 *Id.* at 1116.
- 133 *Id.*
- 134 *Robinson*, 47 Cal 4th at 1119-20.
- 135 See *Robinson*, 47 Cal 4th at 124-26.
- 136 *Id.* at 1125.
- 137 *Id.* at 1126.
-



Publicly Available Websites for IT Lawyers

Following are some publicly available websites relating to varying aspects of information technology law practice. Some of these websites may require payment for certain services. Neither the State Bar of Michigan nor the IT Law Section endorses these websites, the providers of the website, or the goods or services offered in connection therewith. Rather these websites are provided for information purposes only and as possible useful tools for your law practice.

Please provide any feedback or recommendations for additional websites to michael@gallo.us.com.

Miscellaneous

- http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf - The European Union’s recommendations for a comprehensive approach on personal data protection, as of November 2010.
- http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf - Frequently asked questions relating to transfers of personal data from the European Union or the EEA to third countries. Includes a section on ‘Binding Corporate Rules’ for use by multinational organizations
- <http://www.privacyrights.org> – ‘Privacy Rights Clearing House’ is a nonprofit consumer organization with a two-part mission – consumer information and consumer advocacy.
- <http://epic.org> – ‘Electronic Privacy Information Center’ is a public research center that was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment and constitutional values. EPIC publishes a newsletter on civil liberties in the information age.
- <http://www.futureofprivacy.org> – ‘Future of Privacy Forum’ is a think tank that seeks to advance responsible data practices.
- <http://www.idtheftcenter.org> – ‘Identity Theft Resource Center’ is a nonprofit organization dedicated to understanding and prevention of identity theft. ■

Meet a Section Member: **Jeanne Moloney**



Jeanne Moloney

Dykema Gossett PLLC
39577 Woodward Ave
Ste 300
Bloomfield Hills, MI 48304

P: (248) 203-0775
F: (248) 203-0763
E: jmoloney@dykema.com

■ **What is the name of your firm/corporation/employer**
Dykema Gossett PLLC

■ **What is your area of practice?** Corporate Finance, with an emphasis on Technology Transactions

■ **When did you first become involved with the Section?**

When I was a summer associate between my second and third years of law school, I attended a Section event at Andiamo in Novi. I had a great time, and was interested to learn that so many attorneys practiced in more “niche” areas, rather than just general corporate, litigation, etc.

■ **Where did you grow up?**
Livonia, MI

■ **Where else have you lived?** Ann Arbor, MI (during undergrad), Seattle, WA (while interning at Microsoft), Keego Harbor, MI (while teaching high school), New Haven CT (while attending a graduate program), Toledo, OH (law school), Plymouth, MI (currently)

■ **Where did you attend undergraduate and law school?**
Undergrad: University of Michigan, Ann Arbor; Law School: University of Toledo

■ **What was your undergraduate major?** Computer Science Engineering, with a minor in Theatre Arts (very typical, I know)

■ **What are your hobbies, other interests?** I have a huge family (including my husband, two cats, and LOTS of cousins) with whom I enjoy spending time. I also enjoy reading, movies, cooking, and organizing (anything I can label or color code makes me happy). My favorite hobby is probably searching out great deals when shopping.

■ **Favorite restaurant?** Tandoor – a fabulous Indian restaurant in Toledo.

■ **A recent book you read?** The most memorable book I’ve read recently was *The Girl with the Dragon Tattoo*. I know everyone on the planet has read it at this point, but it really is a fascinating read!

■ **Last vacation?** My husband and I spent a few days in the Traverse City area this summer. I hadn’t been to

the area since I was a kid. It’s amazing how beautiful it is up there, and Traverse City is remarkably clean and reasonably priced for such a popular tourist destination.

■ **Favorite legal case (with a tie to Michigan) that can be found in Westlaw or Lexis?** I found the United States v. Rapanos litigation very interesting. I was in law school when the Rapanos civil litigation over alleged Clean Water Act violations was being tried, and our oral advocacy competitions first year were based on that case. In addition, the attorney arguing the case for the US Army Corps in the Supreme Court spoke at our law school. The Supreme Court’s divided opinion in the case demonstrated how complex environmental issues are and continue to be.

■ **Who is your hero?** (a parent, a celebrity, an influential person in one’s life) My mother is my hero. She raised four kids, including one who is severely multiply disabled, and still found the energy to start a non-profit corporation two years ago.

■ **If you had to describe yourself using three words, they would be...** Thoughtful, friendly, organized

■ **What is your favorite movie of the past ten years?** Wow – that’s a surprisingly hard question. Probably *Juno* from the past ten years. My favorite movie ever, though, is *Romy and Michele’s High School Reunion*.

■ **What do you like to do most with a free hour?** When I do have a free hour, I like to catch up on Facebook and see what is going on with friends I don’t get to see often.

■ **What is the most significant event of the last three months?** For me or for everyone? For me, it was probably paying off my student loans(!). In general, it’s hard to say. Possibly the various bank foreclosure “scandals” – they’ve certainly helped to prolong economic recovery.

■ **What one word would you put on your gravestone?**
Fulfilled

■ **A short comment on why you became involved with the Information Law Technology Section:** Mark Malven and Steve Tupper at my firm are very involved with the Section, and I enjoy working with both of them in the technology transactions area. I have also gotten a lot out of the annual IT Law Seminars held in the fall of the past three years, and I hope to become more involved with the Section as my career progresses. ■

2011 Edward F. Langs Writing Award

Essay Competition Rules

1. Awards will be given to up to three student essays, which in the opinion of the judges make the most significant contribution to the knowledge and understanding of information technology law. Factors to be taken into consideration include: originality; timeliness of the subject; depth of research; accuracy; readability; and the potential for impact on the law.
2. Essay must be original, deemed to be of publishing quality, and must not have been submitted to any other contest within the previous 12 months.
3. Essay must be typed, double spaced, at least ten pages in length, must contain proper citations listed as either endnotes or footnotes, and must have left, right, top, and bottom margins of one inch.
4. Essay must include the submitter's name, email address, mailing address, telephone number, and school attended.
5. A total of \$1,500 in US dollars shall be divided between the award winning essays, and all rights to award winning essays shall become the property of the State Bar of Michigan.
6. The Information Technology Section of the State Bar of Michigan reserves the right to make editorial changes, and to publish award winning essays in the Section's newsletter, the *Michigan IT Lawyer*.
7. Essay must be submitted as a Microsoft Word document, postmarked by June 30, 2011, and emailed to dsyrowik@brookskushman.com. ■



Mission Statement—Information Technology Law Section, State Bar of Michigan

The purposes of the Section are to review, comment upon, and appraise members of the State Bar of Michigan and others of developments in the law relating to information technology, including:

- the protection of intellectual and other proprietary rights;
- sale, leasing, distribution, provision, and use of, hardware, software, services, and technology, including computer and data processing equipment, computer software and services, games and gaming, information processing, programming, and computer networks;
- electronic commerce
- electronic implementation of governmental and other non-commercial functions;
- the Internet and other networks; and
- associated contract and tort liabilities, and related civil and criminal legal consequences. ■

