I. INTRODUCTION

Advances in technology are changing the way all of us live and work. In our day-to-day lives, we expect and depend on expedient, if not immediate, world-wide communication and access to information 24 hours a day, seven days a week. The criminal justice community is no exception to the effects of this change. In response to the growing demands on the justice community and its expanding desire and need for information, many states and localities are increasing their information gathering, analysis and sharing capabilities through developing integrated justice information systems. Increasingly, these integrated criminal justice systems allow for instantaneous and seamless access to information within the justice system and with the world at large.

The justice system has been gathering, analyzing, and passing information from one component to another since the "justice process" began. What makes today's automated and seamless sharing of this information different from the "file cabinet and telephone" system of yesterday? This question may have more to do with how society is reacting to the accelerated access and transfer of all types of information, rather than with the justice system process itself.¹

We have yet to determine the effects on an individual's interest in privacy of "too much" information, "easy, instantaneous access" to vast quantities of information, and the analytical capabilities of today's technology. It is to be seen whether the increased access to information and the ability to relate disparate pieces of a person's information results in a distorted and inaccurate picture of that person. Although we have not resolved these questions, it is critical to begin examining

¹While criminal justice agencies traditionally have kept files, automation dramatically changes the nature of such record keeping: there are more individuals as data subjects; there are more data per individual; there is more centralization and correlation of diverse data sources; there is access to the data by more persons; there is faster access to the data; and there is more efficient remote access to the data.)

the unique aspects of gathering, accumulating, analyzing, and sharing information in the justice system and the implications on individual privacy.

Like the medical records area, use of personal information in the justice system carries with it the possibility of irreparable harm to an individual, and therefore, requires a high degree of responsibility from justice agencies. If the concept of privacy focuses on an individual’s capability to control information about him or herself, the question becomes whether the technological capabilities of integrated criminal justice systems to create an analysis or “virtual picture” of an individual that is contained in and used by the criminal justice system violates an individual’s interest in privacy by supplanting an individual’s control over his personal information?3

This article describes the concept of integrated justice systems, how such systems allow justice agencies to gather, accumulate, and analyze various types of information to create a “virtual picture” of an individual which may be shared by the components of the criminal justice system. This article further explains that decision-makers in the criminal justice process may use these “virtual pictures” to make judgments about individuals. This article then determines whether federal law provides rules governing the responsible use by justice agencies of such information or whether “responsible use” rules should be pursued. Part II of this article defines Integrated Justice Systems. Part III defines the various types of information contained in automated justice systems and discusses the differences between criminal history information, 

2. See Fried, Privacy, 77 YALE L.J. 475, 482-83 (1968); Tom Gerety, Redefining Privacy, 12 HARV. C.R.-C.L. L. REV. 233, 281 (1977). Professor Fried argues that a “person who enjoys privacy is able to grant or deny access to others” of information about him or herself. Fried, supra, at 482. Professor Fried uses the example of a house to explain his point. Id. at 483. One’s house is private because the law allows individuals to exclude others from the house, and the “house is constructed - with doors, windows, window shades - to allow it to be made private.” Id. Professor Fried also makes a distinction between simple control over the quantity of information and control over the quality of the knowledge. Id. “We may not mind that a person knows a general fact about us, and yet feel our privacy invaded if he knows the details.” Id.

Professor Gerety argues that “[p]rivacy is . . . the control over the autonomy of the intimacies of personal identity,” Gerety, supra, at 281. Professor Gerety distinguishes privacy from confidentiality. See id. at 282. Private information “excludes all but such information as is necessary to the intimacies of our personal identities.” Id. Confidentiality, however, is created through either “implicit or explicit mutual agreement” and does not depend on the type of information. Id.

This concept of privacy as an individual’s capability to control information about him or herself has also been referred to as “database privacy.” Frederick Schauer, Internet Privacy and the Public-Private Distinction, 38 JURIMETRICS J 555, 556 (1998). Professor Schauer defines “database privacy” as “the purported right of individuals to control the distribution and availability of information about themselves that may appear in various governmental and nongovernmental databases.” Id.

3. An argument may be made that where a state violates an individual’s privacy by disclosing personal information about that individual to the public, the state has deprived the individual of the opportunity to define him or herself. See Francis S. Chlapowski, Note, The Constitutional Protection of Informational Privacy, 71 B.U. L. REV. 133, 154-55 (1991). This author grounds his argument in Professor Fried’s theory that privacy is “control over knowledge about oneself.” See id. at 154-55 & 154 n.147 (1991) (citing Fried, supra note 2, at 483).

Professor Gerety explains that violations of informational privacy depend on how the information is used rather than on how the information is obtained. See Gerety, supra note 2, at 283. He further notes two significant vices latent in the very collection of . . . information: first, there is the possibility, virtually a certainty in many cases, that its life as information will be prolonged beyond necessity or justification; and second, there is the possibility that its contents will be divulged without our consent or knowledge and so without our corrections.

Id. at 287.

Professor Schauer argues that new advances in technology, such as the Internet, “would present a danger to privacy if the Internet only increased the ease and thus the frequency of access to otherwise private information, even if such information was previously accessible, but accessed only rarely.” Schauer, supra note 2, at 558.
criminal intelligence information, juvenile justice information, and a new type of information - supplemental information. Part IV examines whether the capability of an integrated criminal justice system to gather, accumulate, analyze, and share information creates privacy issues requiring further discussion. Part V reviews federal constitutional privacy principles and the privacy principles articulated by federal regulations governing criminal intelligence information and criminal history information. We argue that the outcome of this review demonstrates that the privacy issues raised by integrated justice systems' capabilities are neither addressed by the current federal constitutional privacy law nor by the various federal regulations. This lack of governing privacy principles, we argue, requires a new discussion concerning “What responsible use of criminal justice information within an Integrated Justice System should be.”

II. INTEGRATED JUSTICE SYSTEMS

Integrated justice information systems encompass a variety of information sharing strategies and technologies. In their basic form, they allow justice system agencies (law enforcement, courts, prosecution, defense, corrections, and probation and parole) to input data once, at the place of origin, and seamlessly access and share data with other justice system agencies as the data is passed through the justice system.

For example, when law enforcement arrests a person, the law enforcement agency enters the arrestee’s personal information (name, address, social security number, etc.) into its operational “booking” system. Increasingly, law enforcement agencies have the capability to capture electronic fingerprints, or livescan prints, and add them to the booking system record as well. In addition, the offender’s prior criminal history record (if any) is accessed from the state repository and added to this offense record. This record of information, including the personal information, fingerprints, offense charged, and criminal history, is “pushed,” (automatically electronically transferred) to the next agency in the justice process. Depending upon the jurisdiction, this agency will be the court, pretrial services, or the prosecutor and defender. Each of these agencies in turn adds information to the record and “pushes” it on to the next component agency. In a completely integrated justice system, this “e-record” will be electronically available to many component agencies of the justice system including law enforcement, prosecutors, and the judge in the courtroom when he or she is determining a sentence for the convicted offender. Additionally, this e-record, including the case disposition, will be used to update the offender’s criminal history record, and it will continue on to the correctional institution, where additional information is added during the time the offender serves his or her sentence. Upon release of the offender, critical information on terms of release will be “pushed” to the probation or parole officers and to law enforcement and victims notification systems, where appropriate.

This scenario describes only the most basic processes of the justice system. In reality, the scenario is much more detailed and complex, with information moving forward and backward to various justice system agencies at prescribed times throughout the process. Increasingly, integrated justice systems allow component agencies to interface with public electronic sources, such as the Internet, and other governmental agencies, such as social services, education, and health and welfare. Through these interfaces, the justice system can gather information that may travel through the justice process as well. At each information exchange and access point described above there is an important occurrence: the ability of a human decision-maker accessing the record to gather and analyze data and make critical judgments about the individual whose information is contained in the record.

III. THE INFORMATION
Policy, regulation, and law associated with gathering, storing, and sharing criminal justice information traditionally has focused on three specific types of information: the criminal history record, criminal intelligence information, and juvenile justice information. With the new capabilities of technology, supplemental information is entering the integrated justice system with these more traditional types of information.

A. Criminal History Information

Criminal history records contain distinct pieces of information generated by the criminal justice process. Generally, a criminal history record will contain information identifying the individual, information about any of the individual’s arrests, and “disposition data.” Disposition data commonly includes information about final decisions or actions that terminate the case, including, police decisions to drop all charges, prosecutor decisions not to prosecute, and court acquittals, or convictions and sentences, incarceration, and release.

Automated criminal history records reside in state and federal repositories that can be queried by authorized state and local agencies for criminal justice and non-criminal justice purposes.

Constitutional and common law privacy issues associated with the automated criminal history record have been reviewed since its inception in the early 1970’s, but generally have had little impact on restricting the collecting, storing, and dissemination of criminal history data. Rather, criminal history records systems operate under a patchwork of federal and state statutes and regulations, such as Title 28 Code of Federal Regulations, part 20. Privacy issues


5. See id. “Criminal history record” is defined by Federal regulations as “information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notation of arrests, detentions, indictments, information, or other formal criminal charges, and any disposition arising therefrom, sentencing, correctional supervision, and release.” 28 C.F.R. § 20 (1998).

6. See id. at 1-2 (explaining that each state operates a central criminal history record repository that receives information from justice system components as a case is processed. The repositories compile the information of an individual in to a criminal history record, or “rap sheet.” These rap sheets are available to criminal justice personnel for authorized purposes and to non-criminal justice agencies for purposes such as employment screening and occupational licensing.). Increasingly, state criminal history records include livescan (electronic) fingerprints in addition to the individual’s name and identifying information.

7. See id. at 35 (noting that privacy doctrines of the Federal constitution and common law have been applied to the automated criminal history record systems, but that “constitutional privacy principles do not limit dissemination by criminal justice agencies of information about official acts, such as an arrest... [and so]verge on immunity, civil and official immunity and the need to show tangible harm arising from the alleged misuse of the criminal history record pose insurmountable obstacles to most common law actions by record subjects.”). See also SEARCH Group, Inc., Technical Memorandum No. 12: Criminal Justice Information: Perspectives on Liability, 5-20 (1977); Robert R. Belair and Paul L. Woodward, SEARCH Group, Inc., Case Law Digest: Court Decisions on the Handling of Criminal History Records - Summaries and Analysis (July 1981).

8. See SEARCH, Criminal History Record Information, supra note 4, at 35-36 (describing the federal and state statutes and regulations that apply to criminal history records systems); see also, infra Part IV, C (analyzing whether 28 C.F.R. pt. 20 provides rules governing the use of criminal justice information among criminal justice agencies). For example, the Federal Bureau of Investigation’s authority to maintain criminal history records resides in 28 U.S.C. § 534 (1994). Similarly, state and local jurisdictions that use funding provided pursuant to the Omnibus Crime Control and Safe Streets Act of 1968, as amended, are governed by the criminal history record principles of the Act. See id. at 36. These principles require that “collection, storage, and dissemination of such information shall take place under procedures reasonably designed to insure that all such information is kept current therein; ... and that information shall only be used for law enforcement and criminal justice and other lawful purposes.” 42 U.S.C. § 3789g(b) (1994). State and local jurisdictions receiving federal funding for criminal history record information
associated with the criminal history record continue to be the subject of discussion, as public policy and new technologies move to open access to the criminal history record to a wider audience (e.g., public and private automated background checks). 9

B. Criminal Intelligence Information

Criminal intelligence information is not characterized by the type of information collected, but rather by when the information is collected and how the information is used. The information is generally the product of surveillance of suspected criminals or individuals suspected to be involved in criminal enterprises. 10 “Intelligence information is a wide-ranging collection of facts - employment records, bank statements, tax returns, telephone bills, reports of personal associations - which may provide the basis for major criminal prosecutions.” 11 This information is specific to law enforcement for use in tracking possible criminal activity prior to arrest. 12 Historically, intelligence information “leads” have been collected and analyzed by law enforcement officers in tracking and preventing crime in their jurisdictions.

In the early 1970's law enforcement agencies began using the capabilities of computer systems to store and share intelligence information for multi-jurisdictional crime fighting. Notably, the federally supported Regional Information Sharing System (R.I.S.S.) 13 stored and organized criminal intelligence information on a national basis. In response to privacy concerns associated with computerization of intelligence information, the Department of Justice issued a regulation governing the standard for automated collection, storing, and access of intelligence information in federally funded systems. 14

systems are also bound by the requirements of federal regulation 28 C.F.R. part 20, the purpose of which is “to assure that criminal history record information wherever it appears is collected, stored, and disseminated in a manner to insure the completeness, integrity, accuracy and security of such information and to protect individual privacy.” 28 C.F.R. part 20 (1998). In addition to these federal statutes, states have enacted comprehensive criminal history record statutes, many of which provide even more stringent privacy protections that the federal statutes and regulations. See SEARCH, Criminal History Record Information, supra note 4, at 36.

9. The U.S. Department of Justice Bureau of Justice Statistics and The SEARCH Group, Inc. are continuing to analyze privacy issues relating to criminal history records through the National Task Force on Privacy, Technology and Criminal Justice Information, the most recent meeting of which was held on May 11-12, 1999 in Boston, Massachusetts (copy of proceedings on file with author).


11. Id. at 55-56.

12. See SEARCH, Criminal History Record Information, supra note 4, at 7 (noting the distinction between “intelligence” information and “investigative” information. Intelligence information is “information compiled in an effort to anticipate, prevent or monitor possible criminal activity,” where “investigative” information is “information obtained in the course of the investigation of specific alleged criminal acts.”) For purposes of this article, intelligence information includes all information gathered prior to arrest and prior to establishing specific reasonable suspicion of criminal activity. Investigative information includes information gathered prior to arrest, but after specific reasonable suspicion of criminal activity has been established.


Gathering, Analysis, and Sharing of Criminal Justice Information by Justice Agencies: The Need for Principles of Responsible Use

C. Juvenile Justice Information
The American juvenile justice system traditionally has focused on rehabilitation rather than retribution, separating, in many cases, the juvenile offender from the adult criminal justice process. This separate juvenile process and rehabilitative philosophy is reflected in how juvenile justice information is collected, stored, and shared. Historically, juvenile justice records have received a high degree of confidentiality, limited disclosure, and the possibility of being sealed or expunged. Juvenile justice information is maintained by law enforcement, as well as the juvenile court system. In the past, a juvenile arrest records were often created at the discretion of the law enforcement official, based on his assessment of the crime, with no fingerprinting or photographing of the juvenile. Today, most law enforcement agencies have a formalized juvenile referral process that increasingly includes photographing and fingerprinting juvenile offenders pursuant to state law.

In keeping with the traditional sense of rehabilitation, it is estimated that about one half of the referred juvenile cases are resolved informally, with the help of the family, school and counseling agencies, rather than court intervention. Where court intervention is necessary, a unique juvenile justice record and often a unique juvenile justice offender number is maintained by the juvenile court system. It should be noted that juvenile court records often include "legal records," information similar to adult court records, as well as "social records," information about the juvenile's family, medical or mental health history, and information gathered by social service agencies. The traditional notions of sharing juvenile justice records are under review, based upon changes in juvenile policy, and increased information technology capabilities.

integrated criminal justice information systems.

15. See Privacy and Juvenile Justice Records: A Mid-Decade Status Report, Bureau of Justice Statistics, May 1997, NCJ-161255, p. 6 (describing the American juvenile justice system history and development, namely, the Progressive Movement of the early 1800's that lead to the "rehabilitative ideal" to reform the offender, rather than punishing the offense).

16. See id. at 7 (noting, "[t]he juvenile justice recordkeeping system at this state closely paralleled the predominant philosophy of shielding the child.").

17. See id at 15-16 (explaining that "sealing and purging" of juvenile records remains a popular way to allow a juvenile who is not a repeat offender to enter adulthood with a "clean record." Sealing and purging laws are set out by state statute and are more likely to apply to juvenile court records than to information held by law enforcement).

18. See id. at 23 (noting that "[t]he creation of a record customarily depended on variables, including the severity of the crime, the juvenile’s record, the juvenile’s attitude upon arrest, and the police officer’s background and attitude.").

19. See id. (noting that photographing and fingerprinting juveniles is governed by state law which often requires specific age limitations and levels of offense. In addition, state law governs whether such juvenile records are forwarded to state repositories.).

20. See id. at 24.


22. See id. at 8,19-22, 28 (noting the substantial increase in juveniles transferred to adult court, as well as legislative and judicial initiatives designed to increase juvenile justice information sharing within the justice system and with affiliated agencies). It should be noted that when juveniles are prosecuted in the adult system, their record becomes part of the adult criminal justice system and subject only to the protections of adult systems records. See id. at 28.

The unique confidentiality and policy issues associated with juvenile justice information sharing, though beyond the scope of this article, are worthy of significant consideration.

D. “Supplemental Information:” A New Type of Information
The emergence of integrated justice information systems is introducing a new type of shared information. This information differs from criminal history information, in that may be gathered during the justice process, but is not generated by the process itself; differs from criminal intelligence information, in that it may be added to the system of records after an offender is arrested or indicted; and differs from juvenile justice information, in that it is part of the adult justice system. For purposes of discussion, we refer to this information as “supplemental information.”

For example, on its face, the justice information record described in Section II above does not seem to pose a privacy threat. The information was obtained and added in the process of arresting, prosecuting, judging, and incarcerating an offender (criminal history information). The information in the record, however, deserves a closer look. Increasingly justice agencies’ electronic access to non-criminal justice information, such as financial records, tax statements, credit reports, property records, organizational affiliations, and identification of relatives, friends, employers, and associates makes it easy for all types of information to find its way into the criminal justice system process. 25 This type of extra information, or “supplemental information,” is neither criminal intelligence information nor a part of the criminal history record and may not benefit from traditionally afforded protections. Criminal justice agencies now may electronically gather, accumulate, analyze, store, and share supplemental information between agencies and inter-jurisdictionally.

IV. THE “PICTURE": SHOULD WE BE CONCERNED?
New information gathering and analysis capabilities raise the question that because “supplemental information” is available to justice agencies with access to criminal history and criminal intelligence information, should these agencies freely accumulate and analyze these forms of information in the criminal justice process, or does the a criminal justice agency’s unregulated use of this information violate individual privacy? 26 As noted above, information has always been shared in the

25. See Bercu, supra note 1, at 398 (explaining the information gathering capabilities of the United States Treasury Department’s FinCEN system, “FinCEN is a tool for the centralization of information from disparate sources; it matches one fact to another . . . . It is not simply a data base of stored information awaiting retrieval. Rather, FinCEN’s data bases – linked via computer networks to those at other agencies – represent a pool of data to be combed through routinely by vigilant software.”) Although FinCEN is primarily an intelligence system, used for tracking suspects prior to arrest, the “pooled” information gathering capabilities of the system can be employed to the entire justice process. Increasingly, state and local law enforcement agencies are implementing Internet technologies, data warehousing, or federated data bases that allow inter-jurisdictional and inter-agency sharing of “supplemental information” (vs. intelligence or criminal history information) on a particular subject.

26. Commentators have raised this issue in various contexts including whether “[r]ecording conduct not directly related to crime such as an individual’s political association, his credit rating or employment history, for instance, could create a potential for personal or political repression.” Katzenbach, supra, note 10, at 54.
justice system, but this question must be asked because of the capabilities of new technology and the possible privacy implications of these new technological capabilities.

Changes in technology have historically provided the impetus for the evolution of the American concept of information privacy and privacy law. In the past 100 years, technological innovation has enabled us to see farther and hear better, capture and preserve images of people, places, and events, and communicate instantaneously. Many technologies once thought to violate one’s “right to privacy” are common fixtures of modern society which many of us would not choose to live without, i.e., the telephone, the camera, and television.

One of the most noted articles expounding a person’s right to privacy, or the “right to be let alone,” was written in 1890 by Samuel Warren and Louis Brandeis. In this article, the authors explore to what extent a new technology, the camera, threatened a person’s right to preserve his thoughts, sentiments, and personal information – “the right to one’s personality.” The authors are especially concerned that the capability of technology to allow the reproduction of images or sounds without the participation or consent of the individual and the power of the person capturing the image to reproduce and distribute it to society at large would result in privacy violations that surpass traditional legal protections.

Today’s computer technology is raising many of the same questions as photographic technology 100 years ago. Automated, integrated information systems enable computers to compile, analyze, and relate pieces of personal information from disparate sources. Each of these sources may legally hold the disparate pieces of information, but now technology enables each source to share the information without the subject’s consent or even his knowledge. The technology not only enables the components of the justice system to share information, but also enables components of the justice system to accumulate and analyze distinct pieces of information or data about individuals, including criminal history information, criminal intelligence information, and supplemental information. The accumulation and analysis of this data creates a description and likeness of an individual. This electronic description and likeness is a “virtual picture” which can be shared instantaneously with all the components of the criminal justice system, and is available to decision-makers in the criminal justice process, i.e., a law technology has surpassed traditional legal protections, explaining that the “latest advances in photographic art have rendered it possible to take pictures surreptitiously, the doctrines of contract and of trust are inadequate to support the required protection . . . .” Id. at 211.

30. See Jerry Kang, Information Privacy in Cyberspace Transactions, 50 STAN. L. REV. 1193, 1196-1200 (1998) (explaining that through transacting business on the internet, data is generated, and that data may be aggregated to produce profiles of the people associated with the data). Professor Kang notes that “[a]ll these data generated in cyberspace are detailed, computer-processable, indexed to the individual, and permanent.” Id. at 1199. “Moreover, the data collected . . . can be aggregated to produce telling profiles of who we are, as revealed by what we do and say. The very technology that makes cyberspace possible also makes detailed, cumulative, invisible observations of ourselves possible.” Id.

31. See supra Part II (explaining the information sharing capabilities of integrated justice systems).
of criminal activity. The “photograph” of the individual may or may not be accurate, but nonetheless has drawn the individual into the scrutiny of the criminal justice system. Moreover, if the individual is arrested, the information sharing capabilities of integrated justice systems makes available the same broad array of personal information and the “virtual picture” to the prosecutor to formulate his or her case and perhaps to the probation agency and the courts during sentencing.

While no one should doubt the investigative utility to law enforcement of such technology, there remains the question whether the broad information gathering, analysis, and sharing capabilities of justice information systems may violate an individual’s interest in controlling his or her personal information. Such a violation posses the danger that decision-makers in the criminal justice process, i.e., a law enforcement officer, the prosecutor, the judge at sentencing, or a probation officer, may make judgments about an individual based on information accumulated and analyzed within the integrated justice system without that individual’s consent or even knowledge. Therefore, the information gathering, accumulation, analysis, and sharing capabilities of new technology today, just as in 1890, require us to review the adequacy of our existing legal protections in the context of the justice system.32

V. RESPONSIBLE USE PRINCIPLES

As stated earlier, our central focus of inquiry is whether advances in technology, allowing the various components of the criminal justice system to gather, accumulate, and analyze criminal justice information, and then share and disseminate the information among the

32. See Warren and Brandeis, supra note 27, at 211 (stating “now that modern devices afford abundant opportunities for the perpetration of such wrongs without any participation by the injured party, the protection granted by the law must be placed upon a broader foundation.”)
components of the criminal justice system, raises privacy issues which create a need for the legal system to articulate principles of responsible use of this information. Under American Federal law, there are many different strands of the concept of privacy, and commentators have described privacy as "control over knowledge about oneself."  

The concept of privacy includes the right to be free from unreasonable searches and seizures. Articulated in such a manner, an individual's interest in privacy covers that individual's interest in being protected from a governmental agency's ability to obtain information about that individual. In this article, however, we do not attempt to discuss or evaluate whether this information is legally obtained. This article analyzes whether the accumulating, analyzing, and sharing of information, rather than the surveillance activities of criminal justice agencies, violate an individual's interest in privacy. This article assumes, for the sake of argument, that any information obtained by the criminal justice system from private individuals has been obtained legally.

33. Fried, supra note 2, at 482-83.

34. The Fourth Amendment to the United States Constitution requires that 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.

U.S. CONST. amend. IV.

35. A federal agency's information gathering activities are often described as surveillance activities, and the constitutional privacy concerns of such activities have received extensive treatment in the literature. See generally Albert W. Alschuler, Interpersonal Privacy and the Fourth Amendment, 4 N. ILL. U. L. REV. 1 (1983); Bercu, supra note 1; Robert Garcia, "Garbage In, Gospel Out": Criminal Discovery, Computer Reliability, and the Constitution, UCLA L. REV. 1043 (1991); Thomas B. Kearns, Note, Technology and the Right to Privacy: the Convergence of Surveillance and Information Privacy Concerns, 7 WM. & MARY BILL RTS. J. 975 (1999).

The United States Supreme Court has discussed privacy in terms of an individual's interest in "avoiding disclosure of personal matters," and in maintaining "independence in making certain kinds of important decisions." Additionally, the United States Department of Justice has promulgated two federal regulations articulating standards for the collection, storage, and dissemination of criminal history and criminal intelligence information. In this part of the article, we analyze these privacy principles to demonstrate that the privacy rules that exist do not cover, or regulate, the information accumulation, analysis, and sharing activities in which components of the criminal justice system may engage due to the current advances in technology. Through this analysis and the preceding discussion of the integrated justice system, we hope to spark debate concerning the need for principles of responsible use of information in the criminal justice system.

A. Whether a Protected Privacy Interest Exists

In 1977, the Supreme Court in Whalen v. Roe held that a New York statute requiring doctors to report certain drug prescriptions to the State to be entered into a State controlled and operated database did not "on its face, pose a sufficiently grievous threat" to a Constitutionally protected interest in


“avoiding disclosure of personal matters,” or in maintaining “independence in making certain kinds of important decisions.” The plaintiffs in Whalen challenged this New York statute on the grounds that the statute invaded a “constitutionally protected zone of privacy” because of the possibility that information about a patient’s drug use would become publicly known, and thereby some patients would become reluctant to use these drugs “even when their use is medically indicated.”

Later the same year, the Supreme Court held that the Presidential Recordings and Materials Preservation Act did not “unconstitutionally invade” former President Nixon’s right to privacy. In so holding, however, the Court reasoned that the President’s interest in the contents of his personal communications must be balanced “against the public interest in subjecting [these] . . . materials to archival screening” because the former President had a legitimate expectation of privacy in his personal communications. Through the reasoning in Whalen and Nixon v. Administrator of General Services, the Supreme Court articulated a balancing test for determining whether a privacy interest is violated where the individual asserting the privacy interest has a reasonable expectation in the privacy or confidentiality of the materials at issue.

Courts have used this analysis of (1) determining whether an individual has a legitimate expectation of privacy or of confidentiality in information, and (2), if so, whether the government’s interest in the information outweighs the individual’s privacy interest to determine whether governmental data collection activities violate one’s right to informational privacy. Courts have also framed the discussion of whether an individual has a legitimate expectation of privacy in information as whether an individual’s claim that the government has misused information

44. See Paul v. Verniero, 170 F.3d 396, 401 (3d Cir. 1999) (ruling that to determine “whether information is entitled to privacy protection,” a court must determine whether the individual has a reasonable expectation of confidentiality in the information) (citing Fraternal Order of Police v. City of Philadelphia, 812 F.2d 105, 112-17 (3d Cir. 1987)); Pryor v. Reno, 171 F.3d 1281, 1288 n.10 (11th Cir. 1999) (holding that because information found in motor vehicle records is not the sort of information to which individuals have a reasonable expectation of privacy, there is no constitutional right to privacy in motor vehicle records), petition for cert. filed, July 6, 1999 (No. 99-61); Condon v. Reno, 155 F.3d 453, 465 (4th Cir. 1998), cert granted, __ U.S. __, 119 S. Ct. 1753 (1999) (ruling that because “the information found in motor vehicle records is not the sort of information to which individuals have a reasonable expectation of privacy, . . . there is no constitutional right to privacy in the information contained in motor vehicle records”).

The privacy issue in both Condon and Pryor arose in the context of challenges to the Driver’s Privacy and Protection Act of 1994 (DDPA), 18 U.S.C. § 2721, et seq. See Westover supra note 1 (analyzing the decision in Condon of the United States Court of Appeals for the Fourth Circuit). The United States Courts of Appeals for the Fourth and Eleventh Circuits have held that because there is no constitutional right to privacy in motor vehicle records, the DDPA violates either Congress’ authority under section 5 of the Fourteenth Amendment to the United States Constitution or the Tenth Amendment. See Condon, 155 F.3d at 465; Pryor, 171 F.3d at 1288.

Of course the issue of whether the Constitution protects individuals from infringement by a state or by the federal government is distinct from whether the Constitution provides “protection of an individual’s information privacy from invasion from the private sector.” Kang, supra note 30, at 1230 & 1230 n. 156-157 (reasoning that because of the state action doctrine, the Constitution does not protect private sector invasions of privacy, and noting that “it is unclear to what extent the Constitution actually protects information privacy”).

40. Whalen, 429 U.S. at 599-600.
42. Nixon, 433 U.S. at 457.
43. See Nixon, 433 U.S. at 457; Whalen, 429 U.S. at 599-600.
about that individual comes within a constitutionally protected zone of privacy.\textsuperscript{46}

The Supreme Court, in \textit{Paul v. Davis}, reasoned that “zones of privacy” are created by the operation of other specific constitutional guarantees, and these “zones or privacy” impose limits on governmental authority.\textsuperscript{46} Activities within these “zones of privacy” include “matters relating to marriage, procreation, contraception, family relationships, and child rearing and education.”\textsuperscript{47} The Court ruled that the disclosure of an individual’s information, i.e., a state official’s disclosure to the public of that individual’s arrest on a shoplifting charge, is not included in these constitutionally protected zones of privacy.\textsuperscript{46} A year later, however, in \textit{Whalen}, the Court announced that individuals may have an interest in avoiding government disclosure of personal matters.\textsuperscript{49} Thus, \textit{Paul}, \textit{Whalen}, and \textit{Nixon} indicate that while individuals may have a constitutionally protected privacy interest in avoiding disclosure of personal information,\textsuperscript{50} this interest may be outweighed by the government’s interest in the information,\textsuperscript{51} and arrest data, at least information relating to shoplifting charges, is not protected by a constitutional right to information privacy.\textsuperscript{52}

Courts analyzing the \textit{Paul}, \textit{Whalen}, and \textit{Nixon} line of cases have held that there are certain classes of information in which individuals have no reasonable expectation of confidentiality or privacy\textsuperscript{53} and other classes of information in which an individual has a reasonable expectation of confidentiality, but in which the government’s interest in the information has outweighed the individual’s privacy interest.\textsuperscript{54} With respect to criminal history records, courts have held that disclosure of an individual’s status as a sexual offender, information related to sexual abuse charges, and records containing arrest and conviction information are not protected by a constitutional right to privacy.\textsuperscript{55} At least one court has

\begin{itemize}
\item \textsuperscript{45} See Paul v. Davis, 424 U.S. 693, 713 (1976) (holding that a state official’s disclosure to the public of that individual’s arrest on a shoplifting charge does not come within a Constitutionally protected “zone of privacy”). The Court also held that this individual’s claim that he was defamed by a state official’s disclosure to the public of that individual’s arrest record states neither a claim of a violation of “liberty” nor “property” guaranteed against state deprivation without due process of law. \textit{Id.}
\item \textsuperscript{46} Paul, 424 U.S. at 713.
\item \textsuperscript{47} Paul, 424 U.S. at 713.
\item \textsuperscript{48} Paul, 424 U.S. at 713.
\item \textsuperscript{49} Whalen, 429 U.S. at 598-600.
\item \textsuperscript{50} See Whalen, 429 U.S. at 598-600.
\item \textsuperscript{51} See Whalen, 429 U.S. at 598-600; Nixon, 433 U.S. at 457.
\end{itemize}

52. See Paul, 424 U.S. at 713; Whalen, 429 U.S. at 598-600; Nixon, 433 U.S. at 457; see also, Chlapowski, Note, \textit{supra} note 3, at 145-50 (analyzing the Constitutional right to information privacy).

53. See, \textit{e.g.}, Sheetz v. The Morning Call, Inc., 946 F.2d 202, 207 (3d Cir. 1991) (holding that information contained in a police report concerning a wife’s allegations of spousal abuse were not protected by the confidentiality branch of the right to privacy).

54. See, \textit{e.g.}, United States v. Westinghouse Electric Co., 638 F.2d 570, 576, 580 (3d Cir. 1980) (holding that while an employee’s medical records “which may contain intimate facts of a personal nature” are “entitled to privacy protection,” “the strong public interest in facilitating the research and investigations of NIOSH justify this minimal intrusion into the privacy which surrounds the employee’s medical records”).

55. See Paul v. Verniero, 170 F.3d 396, 403 (3d Cir. 1999) (holding that because "arrest records and related information are not protected by a right to privacy," disclosure of an individual’s sex offender status is not protected); Cline v. Rogers, 87 F.3d 176, 179 (6th Cir. 1996) (holding that because "arrest and conviction are matters of public record," criminal histories are not private personal matters entitled to Constitutional protection), \textit{cert. denied}, 519 U.S. 1008 (1996); Nilson v. Layton City, 45 F.3d 369, 372 (10th Cir. 1995) (holding that information
even held that there is no constitutional right to privacy prohibiting the disclosure of juvenile court records to government and social agencies.\textsuperscript{56}

Even police reports containing allegations of spousal abuse communicated to the police by the abused wife are not protected by a right to privacy.\textsuperscript{57} The Court of Appeals for the Third Circuit concluded that the allegations of spousal abuse were not protected because people related to sexual abuse charges and a conviction is not Constitutionally protected private information because “[c]riminal activity is . . . not protected by the right to privacy”).

Commentators have argued, however, that “once released from prison, offenders should reasonably expect that they can keep their criminal pasts private and begin to rebuild their lives.” Caroline Louis Lewis, The Jacob Wetterling Crimes Against Children and Sexually Violent Offender Registration Act: An Unconstitutional Deprivation of the Right to Privacy and Substantive Due Process, 31 HARV. C.R.-C.L. L. REV. 89, 96-97 (1996).

---

56. J.P. v. DeSanti, 653 F.2d 1080, 1090 (6th Cir. 1981); but see 28 C.F.R. § 20.21(d) (proscribing the “dissemination of juvenile records to non-criminal justice agencies except as provided by a statute, court order, rule, or court decision specifically authorizing the dissemination of juvenile records” and except as provided by 28 C.F.R. § 20.21(b)(3)-(4)). At issue in J.P. was the compilation and potential for disclosure by Cuyahoga County, Ohio court probation officers of juvenile information the “probation officer thinks is relevant to the disposition of a case before the court” including, social histories containing “information form a number of sources, including the complaining parties, the juveniles themselves, their parents, school records, and their past records in the juvenile court,” and information about other members of the juvenile’s family. 653 F.2d at 1082. These social histories are kept on file after the conclusion of a juvenile’s case and are “available to 55 different government, social and religious agencies that belong to a ‘social services clearinghouse.’” Id. The court concluded that “[t]he interest asserted . . . in nondisclosure of juvenile court records, like the interest in nondisclosure at issue in Paul v. Davis, is ‘far afield’ from those privacy rights that are ‘fundamental’ or implicit in the concept of ordered liberty” Id. at 1090.


---

58. Sheetz, 946 F.2d at 207. The court was careful to distinguish the “police’s interest in the privacy of the information [from] . . . the individual’s interest in the information he or she reports.” Id. at 207 n.6. The court noted that “the police may have an interest in keeping investigative information private,” and “may protect this interest by appropriate regulation.” Id.


60. Pryor, 171 F.3d at 1288 n.10. The court ruled that it “acknowledged a constitutional right to privacy only for intimate personal information given to a state official in confidence.” Id.

61. See United States v. Westinghouse Electric Corp., 638 F.2d 570, 577 (3d Cir. 1980) (ruling that “an employee’s medical records, which may contain intimate facts of a personal nature, are well within the ambit of materials entitled to privacy protection”).

62. See Plante v. Gonzalez, 575 F.2d 1119, 1134 (5th Cir. 1978) (ruling that a balancing standard is appropriate to determine whether the State of Florida’s requirement that state senators publicly disclose their personal finances violated their interest in privacy); Westinghouse Electric Corp., 638 F.2d at 578; American Fed’n of Gov’t
medical records, the Courts of Appeals for the Second and Fifth Circuits have used this balancing standard to determine whether laws requiring public officials to disclose personal financial records violated the privacy protections of the Constitution. The Court of Appeals for the Third Circuit in Employees v. Department of Housing and Urban Dev., 118 F.3d 786, 793 (D.C. Cir. 1997) (ruling that where the government collects information from prospective employees through security clearance forms, and the information is not disseminated publicly, the individual’s “interest in protecting the privacy of the information sought by the government is significantly less important” than if the information would be publicly disseminated).

In Plante, the Court of Appeals for the Fifth Circuit held that Florida’s law requiring public disclosure of state senators’ personal finances does not violate the Constitution’s protection of privacy because the “public interest supporting public disclosure” outweighs these elected official’s interest in financial privacy. Plante, 575 F.2d at 1136. The court reasoned that Florida law advances four important state concerns: “the public’s ‘right to know’ an official’s interests, deterrence of corruption and conflicting interests, creation of public confidence in Florida’s officials, and assistance in detection and prosecuting officials who have violated the law.” Id. at 1134-35. These concerns, the court concluded, outweigh the Florida senators’ interest in financial privacy. Id. at 1135-36.

The Court of Appeals for the Third Circuit in Westinghouse Electric Corp. identified seven factors to be considered in determining whether an intrusion into an individual’s privacy is justified: (1) “the type of record requested;” (2) what information the record contains or might contain; (3) “the potential for harm in any subsequent nonconsensual disclosure;” (4) “the injury from disclosure to the relationship in which the record was generated;” (5) “the degree of safeguards to prevent unauthorized disclosure;” (6) “the degree of need for access;” and (7) “whether there is an express statutory mandate, articulated public policy, or other recognized public interest militating toward access.” 638 F.2d at 578.

The Constitution includes a right to informational privacy. The federal constitutional right to informational privacy does not cover most arrest and conviction data and most other types of publicly available information. With the exception of financial information and medical records, courts have yet to address whether “supplemental information” is entitled to privacy protection. Even in the narrow set of circumstances in which a constitutional privacy interest exists, however, that interest may be outweighed by the government’s interest in the information. Thus, the federal constitutional right to informational privacy does not cover the criminal justice system’s capability to accumulate, analyze, and share criminal justice information. Criminal justice agencies may use the integrated justice systems to accumulate, analyze, and share information to create a “virtual picture” of an individual and to share that “virtual picture” with other components of the criminal justice system with minimal concerns of violating an individual’s constitutional right to informational privacy.

---

63. See Barry v. City of New York, 712 F.2d 1554, 1559-61 (2d Cir. 1983) (holding that a provision of New York City’s financial disclosure law permitting public inspection of annual financial reports required of certain city employees did not violate the confidentiality strand of the right to privacy); Plante, 575 F.2d at 1134; but see United States v. Miller, 425 U.S. 435, 442 (1976) (holding that an individual does not have a “legitimate expectation of privacy” in the contents of either checks and deposit slips or the microfilm copies of these checks and deposit slips held by a bank).

64. See Paul v. Verniero, 170 F.3d 396, 404 (3d Cir. 1999) (holding that the New Jersey’s interest in the public “knowing where prior sex offenders live so that susceptible individuals can be appropriately cautioned,” was compelling enough to justify the intrusion).
B. Criminal Intelligence Systems
The United States Department of Justice, Office of Justice Programs (OJP) promulgated a regulation “to assure that all criminal intelligence systems operating through support under the Omnibus Crime Control and Safe Streets Act of 1968, as amended, . . . are utilized in conformance with the privacy and constitutional rights of individuals.” An agency operating an intelligence system covered by these regulations may “collect and maintain criminal intelligence information” about an individual or about the “political, religious or social views, associations, or activities” of individuals, groups, or organizations only if there is “reasonable suspicion” that the individual, group, or organization is “involved in criminal conduct or activity.” The information collected or maintained about an individual must also be “relevant” to the criminal conduct or activity. Information collected or maintained concerning groups or organizations must be “directly related to the criminal conduct or activity.”

The regulation, however, narrowly defines the terms “criminal intelligence information” to include only data which has been evaluated to determine that it (i) is relevant to the identification of and the criminal activity engaged in by an individual who or organization which is suspected of involvement in criminal activity, and (ii) meets criminal intelligence system submission criteria.

Thus, only that data which falls within the definition of “criminal intelligence information” is subject to regulation by 28 C.F.R. pt. 23. Information or data which does not fall within this definition may be collected and maintained by law enforcement agencies in non-criminal intelligence databases without regard to this regulation. Moreover, the regulation applies only to those criminal intelligence systems operating with federal financial assistance provided by the OJP. The regulation, by its terms then, does not apply to those systems not funded by OJP and its component organizations.

While 28 C.F.R. pt. 23 regulates criminal intelligence information if that information is held by an organization receiving federal financial assistance from the OJP for its criminal intelligence system, the regulation does not provide rules for the sharing, accumulation, and analysis among criminal justice agencies of other types of criminal justice information or of any information if the agency does not receive assistance from OJP for a criminal intelligence system. As with the constitutional right to informational privacy, this regulation does not cover the ability of criminal justice agencies to accumulate, analyze, and share information to create a “virtual picture” of an individual and to share this “picture” with other components of the criminal justice system.

C. Criminal History Record Information Systems
OJP also promulgated regulations to “assure that criminal history record information wherever it appears is collected, stored, and disseminated in
a manner to insure the completeness, integrity, accuracy and security of such information and to protect individual privacy.\textsuperscript{72} These regulations require states to submit to the OJP a plan for operational procedures of criminal history record information systems.\textsuperscript{73} The regulations describe requirements to assure (1) that criminal history record information is complete and accurate;\textsuperscript{74} (2) that dissemination of “nonconviction data” is limited to only those authorized recipients of the data;\textsuperscript{75} (3) that criminal history record information disseminated to “noncriminal justice agencies” shall be used only for the purposes for which the information was disseminated;\textsuperscript{76} (4) that states conduct annual audits to insure compliance with the regulations;\textsuperscript{77} (5) that security standards are established by each state;\textsuperscript{78} and (6) that, for purposes of accuracy and completeness, individuals retain certain rights of access and review of criminal history information.\textsuperscript{79} None of these regulations, however, prohibit the sharing of criminal history information among criminal justice agencies.\textsuperscript{80}

Thus, 28 C.F.R. pt. 20 does not cover the accumulation, analysis, and sharing of criminal justice information among criminal justice agencies. This regulation, therefore, does not protect individual privacy from the criminal justice system’s ability to create a “virtual picture” of him or her, and to share that picture among the components of the criminal justice system.

VI. AN OPENING FOR A NEW DISCUSSION

Under Federal Constitutional privacy principles, while some protection exists, this protection does not cover the accumulation, analysis, and sharing of criminal justice information within an integrated justice system.\textsuperscript{81} The federal regulations governing criminal intelligence systems and criminal history information regulate a narrow scope of issues that similarly does not cover this “virtual picture making” capability of the integrated justice system.

\textsuperscript{72} 28 C.F.R. § 20.1. The OJP has a duty under section 812(b) of the Omnibus Crime Control and Safe Streets Act of 1968, as amended, to “assure that the security and privacy of all [criminal history] information is adequately provided for and that information shall only be used for law enforcement and criminal justice and other lawful purposes.” 42 U.S.C. § 3789g(b). This provision is “administrative in nature” and imposes an “obligation” on the OJP “to assure that the information is used only for the purpose for which it was collected.” Polchowski v. Gorris, 714 F.2d 749, 751 (7th Cir. 1983) (holding that a private action may not be maintained under 42 U.S.C. § 1983 for alleged violations of section 3789g(b)).

\textsuperscript{73} 28 C.F.R. § 20.21.

\textsuperscript{74} 28 C.F.R. § 20.21(a).

\textsuperscript{75} 28 C.F.R. § 20.21(b).

\textsuperscript{76} 28 C.F.R. § 20.21(c).

\textsuperscript{77} 28 C.F.R. § 20.21(e).

\textsuperscript{78} 28 C.F.R. § 20.21(f).

\textsuperscript{79} 28 C.F.R. § 20.21(g)

\textsuperscript{80} The “general policies on use and dissemination” does not prohibit the sharing or dissemination of criminal history information among criminal justice agencies. See 28 C.F.R. § 20.21(C). Rather, the section limits the dissemination to noncriminal justice agencies to the purpose for which the information was disseminated. See id. Moreover, the dissemination of “nonconviction data” is limited to “[c]riminal justice agencies for purposes of the administration of criminal justice and criminal justice agency employment.” Id. § 20.21(b)(1). The regulations define “criminal justice agency” as

(1) Courts;

(2) A governmental agency . . . which performs the administration of criminal justice pursuant to a statute or executive order, and which allocates a substantial part of its annual budget to the administration of criminal justice. 28 C.F.R. § 20.3(c).

\textsuperscript{81} See supra part V., A. (discussing whether a constitutional privacy interest exists).
Thus, criminal justice agencies are largely unfettered in their ability to accumulate, analyze, and share information within the integrated justice system and to create and share with other criminal justice agencies “virtual pictures” of individuals that may or may not be completely accurate.

Most people would not object to law enforcement and the criminal justice system using technology to conduct appropriate investigations to remediate criminal activity. Most, however, would express reservation concerning whether law enforcement should have the unfettered ability to gather, accumulate, analyze, and share intimate personal information concerning individuals not otherwise suspected of criminal activity. This new capability of the criminal justice agencies to use integrated justice systems to create and share with other justice agencies “virtual pictures” of individuals may offend notions of privacy as control over information about oneself because the new technological capability supplants individuals’ control of their personal information. The ability of these systems to accumulate, analyze, and share data to create a “virtual picture” may cause decision-makers in the justice process, e.g., law enforcement officers, prosecutors, judges, and probation officers, to raise suspicions about individuals or organizations that would not be raised were it not for the new technological capabilities of the justice system. While such a capability has obvious benefits for law enforcement and for other branches of the criminal justice system, a discussion must begin to articulate principles of responsible use of this information.

82. See supra Part V., B-C. (analyzing federal regulation of criminal intelligence information and criminal history information).

83. See generally Fried, supra note 2; Gerety, supra note 2.

AUTHORS

Paul F. Kendall, General Counsel for the Office of Justice Programs (OJP), is the Executive Chairman of OJP’s Information Technology Executive Council, as well as Chairman of the Executive Council’s Inter-governmental Information Sharing Working Group, the Intelligence Systems Policy Review Board, and the Privacy Task Force. Mr. Kendall is leading a variety of efforts in developing state and local coordinated information technology programs, and is leading the Intelligence Systems Policy Review Board’s examination of legal and public policy issues associated with information sharing. Prior to his arrival at the Office of Justice Programs, Mr. Kendall held positions of Senior Counsel at the Federal Mine Safety Board, and Assistant General Counsel of the Legal Services Corporation, as well as other positions in public and private practice. Mr. Kendall received his Bachelor of Arts from Columbia College of Columbia University, his Masters in Business Administration from the University of Maryland, and his Juris Doctor from The Catholic University of America, Columbus School of Law. Publications include Legislation: A New Design for Justice Integration, 30 McGeorge L. Rev. 9 (1998).

Neal J. Swartz is an Attorney-Advisor for the Office of Justice Programs (OJP). Mr. Swartz practices in the areas of Administrative Law, Grant and Appropriations Law, and Employment and Labor Law; and Mr. Swartz participates on the OJP Intelligence Systems Policy Review Board and the Department of Justice Privacy Task Force, Subcommittee on Information Collection and Analysis. Mr. Swartz received his Bachelor of Arts in Economics and Philosophy from the University of Notre Dame and his Juris Doctor, cum laude, from the Catholic University of America, Columbus School of Law, where Mr. Swartz was an Editorial Assistant of the Catholic University Law Review.

Anne E. Gardner, Attorney-Advisor for the Office of Justice Programs (OJP), is the co-chair of the Office of Justice Programs’ Integrated Information Sharing Working Group, Intelligence Systems Policy Review Board, and Privacy Task Force. Ms. Gardner also supports OJP’s participation in the Vice President’s Global Criminal Justice Information Network Advisory Committee, the National Performance Review/DOJ Crime Mapping Task Force, and the Department of Justice Privacy and Security Task Force. Ms. Gardner received her Bachelor of Science from the University of Wisconsin at Madison and her Juris Doctor, cum laude, from The Catholic University of America, Columbus School of Law. Publications include Legislation: A New Design for Justice Integration, 30 McGeorge L. Rev. 9 (1998).