UIC John Marshall Journal of Information Technology & Privacy Law

Volume 16
Issue 3 *Journal of Computer & Information Law - Spring 1998*

Article 4

Winter 1997

On-Site Fingerprinting in the Banking Industry: Inconvenience or Invasion of Privacy, 16 J. Marshall J. Computer & Info. L. 597 (1998)

Patrick J. Waltz

COMMENTS

ON-SITE FINGERPRINTING IN THE BANKING INDUSTRY: INCONVENIENCE OR INVASION OF PRIVACY

I. INTRODUCTION

Check fraud accounts for approximately $10 billion per year in lost revenue to the banking industry.[1] In response to this tremendous loss, the banking industry has sought new methods for combating check fraud.[2] Many banks across the nation have implemented an on-site fingerprinting process, which requires customers to undergo fingerprinting when cashing checks.[3] Some critics of on-site fingerprinting agree that the process invades privacy.[4]

---

1. *See* Patricia Sabatini, *PNC Wants Thumbprint on Checks,* PITTSBURGH POST-GAZETTE, July 11, 1997, at D1. Technology has given criminals an edge in crimes of fraud. *See id.* Access to high tech laser printers enables criminals to produce phony checks, drivers licenses, and other documents. *See id.* Aside from laser printers, criminals only need a consumer's checking account number to produce fraudulent checks. *See id.* The combination of a laser printer and an actual checking account number produces a very authentic looking document in about ten minutes. *See id.* These checks are almost indistinguishable from the real thing, and have resulted in an estimated ten billion dollars per year in lost revenue to the banking industry. *See id.*

2. *See id.* When it comes to fighting check fraud, law enforcement agencies are understaffed and can no longer effectively deal with the problem. *See id.* Because of the lack of resources, police have encouraged banks to take their own steps to deter check fraud. *See id.*

3. *See* Ken Stammen, *Area Banks Turn to Thumbprint Ids,* SCRANTON TIMES, July 13, 1997, at C6. On-site fingerprinting (or similar methods) of non-account customers is taking place in thirty states. *See id.* Many of those states have experienced a decrease in cases of check fraud. *See id.* There are two reasons for the decrease in fraud: first, the requirement of fingerprinting deters would-be criminals from attempting fraud; and second, the fingerprint provides law enforcement officials with an incriminating piece of evidence which directly ties the criminal to the criminal act. *See id.*

4. *See* H.G. Reza, *2 Forms of ID, Please and a Thumbprint Retail: Some O.C. Merchants are Fighting Bad Checks by Fingerprinting Their Customers,* L.A. TIMES, Nov. 5, 1996, at A1. Privacy rights groups across the nation received phone calls from many displeased customers. *See id.* Representatives of a San Diego based privacy rights group said

However, the banking industry argues that this new system is necessary in order to reduce check fraud.[5] The industry argues that this new procedure will reduce fraud by deterring criminals from committing the crime and assist in capturing those who have committed it.[6]

Bank customers are concerned that this new procedure invades personal privacy. Fingerprinting is often associated with our criminal justice system.[7] Obviously, people do not want to be treated like criminals, especially when making simple transactions.[8] It is argued that subjecting people to fingerprinting creates a presumption of guilt, thus affecting one's dignity.[9] Furthermore, fingerprinting is a way of disclosing one's identity. Requiring citizens to disclose their identity is very personal, and may invade privacy rights protected by the United States Constitution.

Personal privacy is not only protected by common law doctrines, but it is also a fundamental United States Constitutional right.[10] The Framers of the Constitution believed that it was imperative to protect personal freedoms such as individual privacy, therefore they created the Bill of Rights. Aside from the fundamental right to privacy, other branches of the law protect privacy through common law doctrines.[11] A number of personal interests are protected by privacy law, but the focus of privacy

---

that the process not only makes people feel like they are being treated like criminals, but that it is an invasion of privacy as well. *See id.* Furthermore, privacy rights groups argue that there is already enough information about people on the Internet and a fingerprint will just make it easier for criminals to steal someone's identity. *See id.*

5. *See* Stammen, *supra* note 3, at C6.

6. *See id.*

7. *See Finger Image Identification to Facilitate Electronic and Alternative-Channel Banking* (visited Sept. 3, 1997) <http://www.nrid.com/alt_banking.html>. The public's association of fingerprinting with criminal activity is a formidable relationship to overcome. *See id.* However, recent technological advancements have lessened this association. *See id.* New devices, such as digital scanners, do not have the same procedural characteristics as criminal fingerprinting. *See id.*

8. *See* Reza, *supra* note 4, at A1.

9. *See* Jennifer Constance, *Automated Fingerprint Identification Systems: Issues and Options Surrounding Their Use to Prevent Welfare Fraud,* 59 ALB. L. REV. 399, 407 (1995). An argument in opposition to the on-site fingerprinting of welfare recipients is that it creates a presumption of guilt. *See id.* This argument is repugnant to our criminal justice system, where there is a presumption of innocence until one is proven guilty. *See id.*

10. *See* Griswold v. Connecticut, 381 U.S. 479, 485 (1965).

11. *See* William L. Prosser, *Privacy,* 48 CAL. L. REV. 383, 389 (1960). Privacy law encompasses four types of invasions, each protecting an intangible interest of the plaintiff. *See id.* The four types of intrusions upon an individual's privacy are: "[i]ntrusion upon the plaintiff's seclusion or solitude, or into his private affairs; [p]ublic disclosure of embarrassing private facts about the plaintiff; [p]ublicity which places the plaintiff in a false light on the public eye; [a]ppropriation, for the defendant's advantage of the plaintiff's name or likeness." *Id.*

law is to preserve the right "to be let alone."[12] The right to privacy goes beyond physical intrusions into property;[13] this premise also encompasses mental intrusions, including personal dignity.[14]

In addition to the possible invasion of privacy, on-site fingerprinting may also discriminate against minorities.[15] Banks generally require non-account holders to undergo on-site fingerprinting.[16] Many non-account holders are minorities who do not have bank accounts due to their income status. Under this theory, proposed state laws which will permit on-site fingerprinting will become subject to an equal protection analysis if they are passed.

This Comment addresses a number of privacy concerns associated with on-site fingerprinting. First, this Comment sets forth the legal basis of privacy law and the equal protection clause of the Fourteenth Amendment. Second, this Comment analyzes constitutionally protected privacy rights with respect to on-site fingerprinting. Third, this Comment addresses the effects of on-site fingerprinting on an individual's dignity and solitude. The fourth part of this Comment addresses possible discrimination issues associated with legislation that supports the use of on-site fingerprinting in the banking industry. The fifth part of this Comment addresses the privacy issues surrounding the accumulation and dissemination of personal information by the government and private entities. Public reaction to on-site fingerprinting and societal benefits of the process are addressed in the final sections of this Comment.

II. BACKGROUND

A. CONSTITUTIONAL PRIVACY LAW

"They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the government, the right to be let alone—the most comprehensive of rights and

12. *Id.* Public disclosure of private facts was designed to protect an individual's reputation. *See id.* at 398. Intrusion was created to protect individual mental solitude. *See id.* at 392. Appropriation does not protect mental solitude, it protects propriety. *See id.* at 406. Appropriation makes sure that an individual has exclusive control of his name and likeness, which are essential elements of his identity. *See id.*

13. *See* THOMAS M. COOLEY, A TREATISE ON THE LAW OF TORTS OR THE WRONGS WHICH ARISE INDEPENDENT OF CONTRACT 29 (2d ed. 1888). The concepts of physical and mental intrusion focus on the premise of an individual's right "to be let alone." *See id.*

14. *See* Samuel D. Warren & Louis D. Brandeis, *The Right To Privacy*, 4 HARV. L. REV. 193, 195 (1890). The scope of privacy law expanded to keep up with technological advancements and a changing society. *See id.* The scope of privacy law was limited to tangible interests but now it covers interests that are intangible as well. *See id.* at 193.

15. U.S. CONST. amend XIV, § 1.

16. *See* Stammen, *supra* note 3, at C6.

the most valued by civilized men."[17] This quote from of Justice Brandeis' dissenting opinion in *Olmstead v. United States* suggests that the framers had strong feelings about preserving personal privacy. If the framers had such strong feelings about privacy why is the word "privacy" missing from the Bill of Rights? Although the word "privacy" does not exist in the Bill of Rights there are a number theories which support the notion that it is implicit in a number of the amendments. One theory is that the amendments have penumbras formed by emanations from the specific guarantees in the text.[18] This theory suggests the existence of rights that are not specifically enumerated in the Constitution.[19] Under this penumbra theory, the right to privacy is necessary in order to exercise rights explicitly stated in the amendments.[20] Under a second theory it is argued that the Ninth Amendment encompasses privacy rights which were not explicitly enumerated in the Constitution.[21] Finally, the Fourteenth Amendment preserves individual privacy as well. Although some theorize that privacy protected by the Fourteenth Amendment is dependent upon the other amendments, it actually stands on its own, preserving ordered liberty.[22] Unlike other amendments, which depend on the Fourteenth Amendment or the Fifth Amendment for enforcement, the Fourteenth Amendment has procedural and substantive qualities.[23]

1. *The Penumbras*

The amendments of the Constitution have penumbras, one of them is the right to personal privacy.[24] These penumbras are necessary in order effectuate the enumerated rights. For example, in *Griswold v. Connecticut*, the defendants were convicted of violating two state statutes which prohibited the use and distribution of contraceptive devices.[25]

17. Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting). Preceding this statement, Brandeis stated the following in summarizing the underlying principles of privacy in the Constitution:

> The protection guaranteed by the [Fourth and Fifth Amendments] is much broader in scope. The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only part of the pain, pleasure and satisfactions of life are to be found in material things.

Id.

18. *See* Griswold v. Connecticut, 381 U.S. 479, 484 (1965).

19. *See id.*

20. *See id.*

21. *See id.* at 487 (Goldberg, J., concurring).

22. *See id.* at 500 (Harlan, J., concurring).

23. *See id.*

24. *See id.* at 484.

25. *Id.* at 480. (quoting CONN. GEN. STAT. § 53-32 (1958)). "Any person who assists, abets, counsels, causes, hires or commands another to commit any offense may be prosecuted and punished as if he were the principal offender." *Id.* "Any person who assists,

Justice Douglas stated that there are guaranteed zones of privacy.[26] For example, the First Amendment states that "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press, or the right of the people peaceably to assemble, and petition the Government for a redress of grievances."[27] Douglas stated that the right of association is a necessary penumbra of these specific rights.[28] The right to peaceably assemble or the freedom of religion can only be exercised through the freedom of association, a privacy right. Privacy rights also emanate from the Third, Fourth, Fifth and Ninth Amendments.[29]

2. *The Ninth Amendment*

Justice Goldberg's concurring opinion in *Griswold v. Connecticut* suggests that the Ninth Amendment has some privacy implications.[30] The Ninth Amendment states that "the enumeration in the Constitution of certain rights shall not be construed to deny or disparage others retained by the people."[31] Goldberg reasoned that the language of the first eight amendments cannot possibly cover all of those personal freedoms that the Framers intended citizens to possess.[32] The Ninth Amendment was intended to cover those rights that were not specifically enumerated.[33] James Madison, who drafted the Ninth Amendment, had feared that rights which were not explicitly stated in the Constitution would not exist unless there was mechanism which implied the existence of other rights.[34] For example, certain privacy rights are deeply rooted in our society but are never mentioned in the Bill of Rights, namely privacy rights associated with marriage.[35] Under Goldberg's theory of privacy,

---

abets, counsels, causes, hires or commands another to commit any offense may be prosecuted and punished as if he were the principal offender." *Id.* (quoting CONN. GEN. STAT. § 54-196 (1958)).

26. *See* Griswold v. Connecticut, 381 U.S. 479, 485 (1965).

27. U.S. CONST. amend. I.

28. *Griswold*, 381 U.S. at 484.

29. *See id.* The Third Amendment prohibits the quartering of soldiers in a citizens house without their consent; the Fourth Amendment gives people the right to be secure in their persons, houses, papers, and effects from unreasonable searches and seizures; the Fifth Amendment gives a person "a zone of privacy which the government may not force him to surrender to his detriment." *Id.*

30. *Id.* at 487 (Goldberg, J., concurring).

31. U.S. CONST. amend IX.

32. *See Griswold*, 381 U.S. at 488 (Goldberg, J., concurring).

33. *See id.* James Madison was responsible for the work of the Ninth Amendment. *See id.* It was theorized that the particular amendments could not possibly specify all individual rights, and to specify some rights might be misinterpreted to only include those rights, thus depriving citizens of unspecified rights. *See id.*

34. *See id.*

35. *See id.* at 491.

this is the type of right that the Ninth Amendment preserves. Ultimately, these rights in the Ninth Amendment, like those in the First, Third, and Fourth, are enforced by the due process clause of the Fifth and Fourteenth Amendments.

3. *The Fourteenth Amendment*

Some Supreme Court Justices also suggest that the Fourteenth Amendment independently preserves privacy rights.[36] Under the previous theories, the right to privacy was found in one or more of the first nine amendments and ultimately, enforced by the Fourteenth Amendment's due process clause. However, under this third theory of constitutional privacy, there are privacy rights protected by the Fourteenth Amendment's due process clause.[37] Under this theory, there are personal liberties that may not be abridged by any state without due process of the law, among those liberties is privacy.[38] Thus, the Fourteenth Amendment stands on its own power; a guarantee of rights and the power to enforce those rights.[39]

State laws or actions that inhibit the exercise of fundamental rights are subject to a very high standard of judicial review. This standard is known as strict scrutiny. Under this standard, states carry the burden of proving a number of things. First, the state must show that the act promotes a compelling state interest.[40] The state must also prove that the interest is narrowly tailored, and that the act is the least restrictive means of accomplishing that interest. If the state fails to meet any of the aforementioned burdens, the act is considered unconstitutional.[41]

B. Tort Based Privacy Law

The preservation of individual privacy is of paramount importance.[42] As mentioned earlier there are a number of constitutional privacy rights, but aside from these constitutional rights to privacy, there

36. *See* Meyer v. Nebraska, 262 U.S. 390, 399 (1923).

37. *See* Griswold v. Connecticut, 381 U.S. 479, 491 (1965) (Harlan, J., concurring).

38. *See id.*

39. *See id.* at 500. There are basic values implicit in the concept of ordered liberty, this concept is not dependent upon any of the first nine amendments, the Due Process Clause of the Fourteenth Amendment stands "on its own bottom." *See id.*

40. *See* Bates v. City of Little Rock, 361 U.S. 516, 524 (1960). "Where there is a significant encroachment upon personal liberty, the State may prevail only upon a showing a subordinating interest which is compelling." *Id.* Laws that are reasonably necessary to effectuate a legitimate state interest are not unconstitutional under the Due Process clause. *See* Zemel v. Rusk, 381 U.S. 1 (1965).

41. *See* Katz v. United States, 389 U.S. 347, 351 (1969).

42. *See* Warren & Brandeis, *supra* note 14, at 193. Technological advancements made in the media and in communications have encroached upon individual privacy. *See id.* Solitude and privacy are a core part of individuality, and intrusions upon solitude subject

are common law doctrines that preserve privacy as well. Interestingly enough, these privacy doctrines have spiraled off from other torts.

Common law battery was created in an attempt to protect individuals from unwarranted physical abuse by others.[43] Assault is a concept which, among other things, seeks to protect individuals from the fear of physical abuse.[44] Ideally, assault affords a remedy to an abused individual for the mental shock his body had to endure in preparing for imminent physical contact.[45]

Privacy rights have stemmed from assault and battery, with the primary focus staying the same: protecting an individual from the unwarranted intrusions of others, whether physical or mental.[46] The principle focus of privacy law is to preserve the right "to be let alone."[47] Samuel D. Warren and Louis D. Brandeis expanded on this concept and laid down the framework of privacy law in their seminal article *The Right To Privacy*.[48] Warren and Brandeis stated that the concept of privacy encompasses more than just tangible property, it includes the simple "right to enjoy life."[49]

This right was the catalyst for the development of tort related privacy laws. With this basic right in mind, William Prosser proposed a number of legal remedies to individuals who have been injured in this respect. Prosser developed four privacy causes of action.[50] Those causes of action are intrusion, public disclosure of embarrassing facts, publicity which places the plaintiff in a false light in the public eye, and appropriation.[51] The basis of these actions affect different aspects of individual dignity. These actions are founded upon injury to an individual's reputation, mental solitude, or propriety.[52]

Like Prosser, Warren and Brandeis believed that the preservation of individual solitude is part of that right to enjoy life and an essential element of individuality.[53] Warren, Brandeis, and Prosser sought to preserve more than dignity, they also sought to prevent the dissemination of

---

individuals to mental pain and distress. *See id.* Often, this pain is "far greater than" that inflicted by "bodily injury." *Id.*

43. *See* COOLEY, *supra* note 13, at 29.

44. *See id.*

45. *See id.*

46. *See id.*

47. *Id.*

48. Warren & Brandeis, *supra* note 14, at 193.

49. *Id.*

50. *See* Prosser, *supra* note 11, at 389.

51. *Id.*

52. *Id.*

53. *See* Warren & Brandeis, *supra* note 14, at 195.

personal information.[54] The process of on-site fingerprinting may threaten both of these aspects of privacy. It is argued that the process of on-site fingerprinting is intrusive and offends personal dignity. It is also argued that retaining this information and then disclosing it to the government or other private entities is unwarranted.

C. The Fourteenth Amendment's Equal Protection Protection Clause

The Fourteenth Amendment specifies that "No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws."[55] If a court determines that a suspect class is denied equal protection of the laws, the court must analyze the discriminating statute with strict judicial scrutiny under this equal protection clause.[56] Courts will hold that statutes which discriminate against suspect classes are unconstitutional.[57] However, there is one exception to this rule. The burden is on the state to prove that the statue serves a compelling state interest and that the statute is the least restrictive means available to further that compelling interest.[58]

A statute is discriminatory on its face if the language of the statute specifically classifies people based upon race and discriminates based upon that classification.[59] State acts that are discriminatory on their face require a different approach. If the statute is not discriminatory per se, but discriminates in its operation, the statue may still be subjected to a Fourteenth Amendment analysis. If the statute only discriminates in its operation, then the element of intent to discriminate must be proven.[60] If it is found that the these two elements are satisfied, then the state must show that the statute is furthering a compelling state interest, and that they are doing so in the least restrictive means possible.

---

54. *See* Prosser, *supra* note 11, at 398. Public disclosure of private facts was intended to protect ones reputation by providing a remedy to those who have experienced mental distress due to the dissemination of those facts to the public. *See id.*; Warren & Brandeis, *supra* note 14, at 198. According to Warren and Brandeis, the common law gave every individual the right to determine what aspects of his personal life were to be communicated to others. *See id.*

55. U.S. Const. amend. XIV.

56. *See* Skinner v. Oklahoma, 316 U.S. 535, 541 (1942).

57. *See* San Antonio Indep. Sch. Dist. v. Rodriguez, 411 U.S. 1, 19 (1973).

58. *See* Bates v. City of Little Rock, 361 U.S. 516, 524 (1960).

59. *See San Antonio Indep. Sch. Dist.*, 411 U.S. at 29.

60. *See* Washington v. Davis, 426 U.S. 229, 240 (1976).

D. Biometrics and On-Site Fingerprinting

1. *Biometrics*

Identifying criminals based upon unique physical characteristics is far from being a new concept.[61] Nevertheless, biometrics has been in use in this country since 1903. The most common form of biometric use is the use of fingerprinting by law enforcement. Although fingerprinting is not the most reliable means of identification, it is certainly the most practical. In addition to criminal identification, many establishments have resorted to biometrics as a security measure. Security is precisely what the banking industry attempted to preserve when many financial institutions implemented on-site fingerprinting programs.

2. *The Process of On-Site Fingerprinting*

The process of on-site fingerprinting is rather simple. The process requires individuals without accounts to undergo fingerprinting in order to cash checks.[62] There are two basic procedures. There is an inkless dye process, where the customer is asked to put his thumb into the dye, then onto the back of the check.[63] The check is then deposited against the account and then put on file at the bank. Sometimes the check will be returned to the writer, or it will be put on file in the bank and a statement will be sent to the writer. The check will remain with the bank until fraud is suspected, then it is turned over to the proper authorities with the suspect's fingerprint on the back.

Digital scanning is the second method of on-site fingerprinting.[64] A digital scanning device reads the customer's fingerprint and copies a few distinguishable characteristics into a database.[65] The computer does not copy the image into the database, the image is transformed into binary

---

61. Joseph Peterson, *Preface* to Alphonse Bertillon, Identification of Criminals (Gallus Muller trans., AMS Press 1977) (1889). One of the oldest methods of scientific identification is called the Bertillon anthropometric system. *See id.* Bertillon measured the body parts of criminals in an attempt to make identification easier. *See id.* Under Bertillon's system, the probability of two people having the same measurements was 4,000,000 to 1. *See id.*

62. *See* Stammen, *supra* note 3.

63. *See* Sabatini, *supra* note 1, at D1.

64. *See* Matt Zoller Sietz, *Debate Over Privacy Lies at One's Fingertips Will Someday Your Prints Come to Haunt You?*, Star Ledger (Newark, N.J.), July 13, 1997, at A1. Another type of fingerprinting device is a digital scanner which stores the print in a computer database for future matching. *See id.*

65. *See* Constance, *supra* note 9, at 401. The finger imaging process scans the fingerprint and extracts identifiable characteristics. *See id.* The system does this in substantial detail in order to distinguish the print from the great number of prints in the database. *See id.* The computer scans the print and converts the "spatial relationship" of the print's ridges into a mathematical representation of the print. *Id.* The data is then converted to binary code which is used in the search. *See id.*

information.[66] Binary data enables the computer to mathematically search the database for matches at a rate of 600 prints per second.[67]

Many states use digital scanners to prevent fraud in their welfare programs.[68] Some states even use a more sophisticated means of digital identification. Retinal eye scanners have been incorporated into some welfare systems. The process is very similar to digital fingerprinting. Instead of placing their fingers on a scanner, the scanner will read the customer's retinal vein pattern. Like fingerprints, vein patterns are very unique. However, unlike fingerprints which may be altered, there is no reasonable way to alter the vein pattern of an eye without serious consequences.

The process of on-site fingerprinting serves two purposes. First, it gives the bank and law enforcement officials some information regarding the customer's identity.[69] Fingerprinting is one of the most accurate means of identification,[70] and it can assist in the identification of those who commit fraud.[71]

In addition to identification purposes, fingerprinting deters criminals from attempting fraud.[72] Potential criminals will think twice before leaving a piece of information at the crime scene which will directly tie them to the criminal act. This theory has proven to be successful in many states where check fraud drastically decreased. For example, one hundred fifty-five financial institutions in Texas have reported a seventy percent decrease in check fraud since the implementation of the program.[73] Other states have had similar results as well. Some states have reported a forty-two percent decrease in check fraud.[74] This tremendous decrease is attributed to on-site fingerprinting.[75] It

66. *See id.*

67. *Id.*

68. *Id.*

69. *See* Sabatini, *supra* note 1, at D1.

70. *See* Tracey E. Kaplan, *Fingerprinting New York State Job Applicants: Invasion Of Privacy,* 25 COLUM. J.L. & SOC. PROBS. 91, 92 (1991). Fingerprinting is one of the most accurate means of identification. *See id.* The accuracy of fingerprinting in combination with its low cost make fingerprinting extremely efficient and one of the most widely accepted methods of identification. *See id.*

71. *See* Stammen, *supra* note 3, at C6.

72. *See* John McCormick, *Turning Thumbs Down on Bad Check Writers,* DES MOINES REG., April 27, 1997, at 1. According to the Iowa Bankers Association, one of the primary reasons why on-site fingerprinting was adopted was to deter attempts of committing check fraud. *See id.*

73. *See* Stammen, *supra* note 3, at C6.

74. *See id.*

75. *See id.* It has also been reported that 155 institutions in Texas have cut fraud by nearly seventy percent since the implementation of the program. *See id.* This decrease in fraud loss was attributed to a pilot program in the state of Texas. *See id.* Additional pilot programs have yielded similar results in Arizona, Utah, and California. *See id.* In addition

does not take a mathematician to figure out that the decrease in check fraud will reduce the banking industry's $10 billion deficit attributed to that crime.

III. ANALYSIS

A. CONSITUTIONALITY OF ON-SITE FINGERPRINTING

The issues surrounding the use of on-site fingerprinting can be divided into two categories. The first category includes jurisdictions which have proposed legislation that will explicitly permit banks to use on-site fingerprinting. The second category encompasses the remaining institutions, those banks that do not have legislative support for their use of on-site fingerprinting, but use it anyway.

The issue surrounding the proposed legislation of some jurisdictions is to determine whether a mandatory fingerprinting is an invasion of privacy, and if so, whether state laws permitting the use of on-site fingerprinting are constitutional under a strict scrutiny analysis. The issue associated with those banks that do not have legislative support is whether they are acting as a state under the state action doctrine, thus subjecting them to the same constitutional analysis as the state laws.

The Fourth Amendment specifically prohibits the government from conducting unreasonable searches and seizures.[76] However, in *Winston v. Lee*,[77] the Supreme Court stated that the Fourth Amendment "protects expectations of privacy, the individual's legitimate expectations that in certain places and at certain times he has the right to be let alone, the most comprehensive of rights and the most valued by civilized man."[78] The Court in *Winston* stated that the right to privacy under the Fourth Amendment, is protected from governmental intrusions up to a specific standard—probable cause.[79] That is the search will be deemed "reasonable" under the Fourth Amendment if the search will advance the community's "vital interest."[80]

It is argued that the privacy right invaded by on-site fingerprinting comes from the Fourth Amendment's search and seizure clause. The Fourth Amendment specifically refers to unreasonable governmental searches and seizures.[81] Typically, preservation of individual privacy

"both the FBI and the Secret Service have testified before Congress about the merits of the programs." *Id.*

76. *See* U.S. CONST. amend. IV.

77. Winston v. Lee, 470 U.S. 753 (1985)

78. *Id.* at 758 (quoting Olmstead v United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting)).

79. *Id.* at 759.

80. *Id.*

81. U.S. CONST. amend. IV.

from other individuals or private organizations, such as a bank, is left to the states.[82] Although some courts extend the search and seizure clauses of state constitutions to encompass intrusions by private entities, the Fourth Amendment only extends to governmental intrusions.[83] The United States Constitution does not extend to purely private entities.

The first issue to be determined is whether fingerprinting is an unjustified invasion of privacy. In *Davis v. Mississippi*,[84] the Supreme Court stated that fingerprinting per se is not a violation of a person's Fourth Amendment right.[85] In making this determination, the Court analyzed the process of fingerprinting and concluded that the process does not probe "into an individual's private life and thoughts that marks an interrogation or search."[86] However, a few aspects of the Court's opinion in *Davis* should be considered. First, this opinion was not the Court's holding in the case, the case was decided on other grounds.[87] Therefore, the statement implying that fingerprinting is not an invasion

82. *See* Katz v. United States, 389 U.S. 347, 351 (1967). "A person's general right to privacy is-his right to be let alone by other people, is like the protection of his property and of his very life, left largely to the law of the individual states." *Id.*

83. *See* Hill v. National Collegiate Athletic Ass'n, 865 P.2d 633, 640 (Cal. 1994). In *Hill,* the plaintiff attempted to prevent the National Collegiate Athletic Association from requiring her to take a drug test. *See id.* at 633. The plaintiff based this argument on California's search and seizure clause, which was taken word for word from the United States Constitution. *See id.* The National Collegiate Athletic Association argued that the provision of the constitution did not apply to them. *See id.* This argument was based on the fact that they were a non-governmental organization and the corresponding provision of the state's constitution was created to protect individuals from governmental invasions. *See id.* The court stated that the state's search and seizure clause extended to violations by private organizations and held that the plaintiff's constitutional rights were violated by the non-governmental defendant. *See id.* at 640.

84. Davis v. Mississippi, 394 U.S. 721 (1969).

85. *See id.* at 727. The defendant was convicted of rape and sentenced based upon fingerprints that were illegally obtained through a forcible seizure. *See id.* at 723. The Supreme Court stated that fingerprinting itself does not violate the Fourth Amendment. *See id.* at 728. However, the court held that the detention of the defendant in police headquarters was unreasonable since there was no probable cause. *See id.* Therefore, the fingerprints were illegally obtained and could not be used to incriminate the defendant. *See id.*

86. *Id.*

87. *Id.* Although the Court addressed the fingerprinting issue in its opinion the court ruled that the defendant's Fourth Amendment rights were violated:

> We have no occasion in this case, however, to determine whether the requirements of the Fourth Amendment could be met by narrowly circumscribed procedures for obtaining, during the course of a criminal investigation, the fingerprints of individuals for whom there is no probable cause to arrest. For it is clear that no attempt was made here to employ procedures which might comply with the requirements of the Fourth Amendment: the detention at police headquarters of the petitioner and other young Negroes was not authorized by a judicial officer; petitioner was unnecessarily required to undergo two fingerprinting sessions.

Id.

of privacy is dicta. The Court did hold that there was a violation of the defendant's Fourth Amendment right, however, that was related to the unreasonable seizure rather than the search.[88]

Second, this statement was made in a criminal context. Obviously, criminals or suspected criminals have a different expectation of privacy than non-criminals, hence bank customers. A person accused of committing a crime expects to be fingerprinted. Therefore, when a fingerprinting is conducted on a suspected criminal there is no invasion of privacy. However, a bank customer has a higher expectation of privacy than a suspected criminal. Obviously, a person entering a bank for the purpose of performing a simple transaction does not expect to be fingerprinted.

One fact about on-site fingerprinting that supports the finding that it does not invade privacy rights associated with the Fourth Amendment is the voluntary nature of the process. Since bank customers have the option of not undergoing fingerprinting, the process could hardly fall under a seizure. Hence, there is no need to "effectuate" a search because the prints are voluntarily provided. Therefore, on-site fingerprinting falls under the latter of the two methods of obtaining fingerprints, a simple search. Customers claim it is this search that invades their privacy and violates their Fourth Amendment right.

However, in *Katz v. United States*,[89] the Court stated that the Fourth Amendment does not protect personal interests which are continuously exposed to the public eye.[90] In *Katz*, recordings of the defendant's voice were used in an attempt to prove his guilt.[91] The defendant argued that the conversations were illegally recorded, and thus protected under the Fourth Amendment.[92] The Court agreed that the defendant's phone calls were private conversations. However, the Court also stated that under ordinary circumstances vocal projections do not warrant Fourth Amendment protection, because one's voice is continuously exposed to the public.[93] The reasoning behind this statement is twofold. First, an

88. *See id.*

89. Katz v. United States, 389 U.S. 347 (1967).

90. *Id.* at 351. In *Katz*, the defendant was convicted of interstate transmission of bets and wages. *Id.* at 348. In trial court, the prosecution was permitted to use evidence of the petitioner's telephone conversations relating to the wagering. *See id.* The defendant argued that the telephone booth in which he conducted business was a constitutionally protected area. *See id.* In rendering the decision, the Court stated that anything people knowingly expose to the public "even in his own home or office, is not subject of Fourth Amendment protection." *Id.* at 351. However, the Court held that the phone booth in which the conversations took place was protected because the defendant made efforts to exclude the public from his conversations and thus expected privacy. *See id.* at 358.

91. *Id.* at 350.

92. *See id.* at 348.

93. *See id.* at 351.

individual has certain expectations of privacy.[94] For example, if a person discloses private facts to the public, that person cannot reasonably expect those facts to remain private. Second, the Court will not protect a person's privacy when that person makes no effort to preserve it themselves.[95] A person who speaks openly in public about a personal matter has not attempted to protect his own privacy in regards to that matter.

The Court's reasoning in *Katz* brings up a number of issues surrounding the expectation of privacy and fingerprinting. It could be argued that an individual does not have a reasonable expectation of privacy in their fingerprints. While in public, people leave their fingerprints on just about everything they touch.[96] One cannot expect their fingerprints to remain private when they constantly display them to the public.

However, unlike vocal projections, fingerprints are not easily detected by the general public. Leaving an invisible fingerprint in public is different than openly speaking about private matters in public. A person who openly speaks about private matters in public is aware that anyone nearby may hear what they are saying. Hence, there is little to no expectation of privacy. However, fingerprints are not visible to the naked eye and can only be recorded by lifting the print with special equipment. This would be the equivalent of using a sensitive listening devise to record personal conversations which are otherwise undetectable by the human ear. This would certainly invade Fourth Amendment privacy rights, as the Court in *Katz* decided.[97]

Since *Davis* and *Katz* essentially deal with privacy rights in a criminal context, it would be wise to explore cases closer to point; cases which deal with fingerprinting in a civil context. In *Thom v. New York Stock Exchange*,[98] the plaintiffs were required by New York State law to undergo fingerprinting as a condition of employment.[99] The plaintiffs argued that the statute was constitutional.[100] The basis of the plaintiffs' argument was that the statute was an invasion of privacy under the Ninth Amendment; punishment without due process of law in violation of the Fourteenth Amendment; and an unequal protection of the law,

94. *See id.*

95. *See id.*

96. WAYNE R. LAFAVE, SEARCH AND SEIZURE § 2.2 (2d ed. 1987).

97. *Cf.* Katz, 389 U.S. at 359.

98. Thom v. New York Stock Exch., 306 F. Supp. 1002 (S.D.N.Y. 1969).

99. *Id.* at 1007. Plaintiffs, employees of the New York Stock Exchange, argued that New York's mandatory fingerprinting of Stock Exchange employees was unwarranted. *See id.* The Court stated that fingerprinting was warranted upon a showing of probable cause or a compelling state interest. *See id.*

100. *See id.* at 1004.

also a violation of the Fourteenth Amendment.[101] The plaintiffs' main contention was that fingerprinting invades privacy, and that fingerprints are a way for the government to control society and an "intrusion upon one's past and future life."[102] Accordingly, the plaintiffs argued that the state must show a strong justification for the intrusion.

The court stated that the fingerprinting was a security measure to ensure that criminals were not hired in this highly sensitive field.[103] The evidence showed that the law was designed to combat a "worsening problem in the securities industry."[104] The court stated that this measure was well within the state legislature's power to reduce thefts, embezzlement, and related crimes. Ultimately, the court concluded that the statute permitting the fingerprinting of employees was constitutional.[105]

Similar to the mandatory fingerprinting in *Thom*, on-site fingerprinting in the banking industry is a security measure. Both banking and finance are industries which involve the handling of money, thus making them highly vulnerable to criminal activity. Due to this high potential for criminal activity, security is of paramount importance and preservation of this field is a compelling state interest. Therefore, under *Thom*, the use of on-site fingerprinting in the banking industry should be justified.

An aspect about the *Thom* decision which strengthens the argument in favor of on-site fingerprinting is the fact that the plaintiffs had no access to securities, hence, they had no access to the very thing that the statute was designed to protect.[106] Nevertheless, the Court ruled that direct access to the securities was immaterial, due to the fact that people in the plaintiffs' positions could conspire to commit the crimes.[107] The court in *Thom* upheld the fingerprinting of people who did not have direct access to the means to commit a crime. Therefore, there is no reason why consumers should not be subjected to on-site fingerprinting when they have direct access to the means to commit a crime. In fact, they are the very people that possess the materials needed not only to conduct the transaction, but to commit fraud as well.

The Fourth Amendment specifically refers to governmental searches and seizures.[108] Typically, preservation of individual privacy from other individuals or private organizations, such as a bank, are left to the states. Some courts extend the search and seizure clauses of state con-

101. *See id.*
102. *Id.*
103. *See id.* at 1006.
104. *Id.* at 1007.
105. *See id.* at 1012.
106. *See id.* at 1009.
107. *See id.*
108. U.S. CONST. amend. IV.

stitutions to encompass intrusions by private entities. However, the Fourth Amendment only extends to governmental intrusions.[109] That is not to say that all private entities are free to violate constitutionally protected privacy rights. In order to subject a private entity to a constitutional analysis under the Fourteenth Amendment's due process or equal protection clauses, the entity must meet certain criteria under the "state action doctrine." Essentially, the "state action doctrine" subjects private entities to a Fourteenth Amendment analysis when they act on the state's behalf, or when their connections with the state are so closely tied as to conclude that they were acting as an agent for the state.[110] This would mean that courts may enjoin private entities from violating constitutional provisions that prohibit state governments from depriving a "person of life, liberty, or property without due process of law."

For the purposes of this Comment, the question of whether banks are subject to the Fourteenth Amendment under the state action doctrine will remain open. It is not necessary to investigate this matter since fingerprinting per se does not invade constitutionally protected privacy rights. The slight invasion is not significant enough to trigger the violation of a fundamental right.[111] Additionally, the process is done on a voluntary basis, essentially acting as a waiver of exercising that specific right. Although the Constitution does not afford a remedy for this invasion of privacy, there may be some meritorious arguments under alternative theories such as discrimination under the equal protection clause, or a tort related remedy.

B. Invasion of Dignity and Solitude

On-site fingerprinting may give people the feeling that they are being treated like criminals, and thus, presumed to be committing check fraud.[112] The basis of this argument is that only suspected criminals are fingerprinted, and since some banks require some customers to be fingerprinted, there is a presumption of guilt.[113] However, this is not a valid

109. *See* Hill v. National Collegiate Athletic Ass'n, 865 P.2d 633, 640 (Cal. 1994).

110. *See* Jackson v. Metropolitan Edison Co., 419 U.S. 345, 350 (1974). In deciding whether a private utility company was subject to the Fourteenth Amendment, the Court stated that private entities will be held subject to that amendment if "there is a sufficiently close nexus between the state and the challenged action of the regulated entity so that the action of the latter may be fairly treated as that of the state itself." *Id.*

111. *See* Davis v. Mississippi, 344 U.S. 721, 727 (1969).

112. *See* Charles O'Hara & Gregory O'Hara, Fundamentals of Criminal Investigation 671 (5th ed. 1981). Fingerprints are a necessary means of criminal identification. *See id.* Typical arrest procedures of criminals involve the taking of fingerprints. *See id.* at 880.

113. *See* Terry v. Ohio, 392 U.S. 1, 20 (1967). In *Terry*, a police officer observed unusual conduct by the defendant. *Id.* The officer theorized that the defendant was about to commit a robbery. *See id.* at 5. The officer approached the defendant and conducted a search based upon his hunch. *See id.* at 6. Upon searching the defendant, the officer found a

argument. First, our criminal justice system fingerprints suspected criminals, but they are always presumed innocent until proven guilty.[114] Therefore, there is not a presumption of guilt. In addition, customers are not being held captive and then forced to undergo fingerprinting. They have the option of doing business elsewhere. In fact, it would be in their best interest to refuse to do business at banks that have a fingerprinting program in affect. Displaying their displeasure in the system may send a message to the banks. If enough customers protest this program the banks may use a different security method ultimately changing their policies.

In addition, the court in *Thom* noted that the link between criminal activity and fingerprinting no longer exists.[115] The court in *Thom* explained that many employers, including the U.S. Government, require fingerprints of their employees.[116] Also, recent technological advancements have altered the fingerprinting process.[117] Civil fingerprinting is

---

revolver in the defendant's pocket. *See id.* The defendant was convicted of carrying a concealed weapon, but he appealed. *See id.* The defendant claimed that the search was not warranted by probable cause. *See id.* at 20. The Court stated that although it is not expressly written into the Fourth Amendment of the U.S. Constitution, searches and seizures are unwarranted without probable cause. *See id.* The Court confirmed that probable cause must be based on something more than hunches, and conducting a search on mere good faith is not enough. *See id.*

114. *See* Constance, *supra* note 9, at 407. "Another argument against finger imaging is that it creates a presumption of guilt, contrary to the basic fundamental premise that an individual is presumed innocent until proven guilty." *Id.*

115. Thom v. New York Stock Exch., 306 F. Supp. 1002, 1008-12 (S.D.N.Y. 1969). In *Thom*, the plaintiff challenged the constitutionality of a New York statute which required all employees "of national security exchanges registered with the Securities and Exchange Commission" to be fingerprinted as a condition of employment. *Id.* at 1004. The court stated that fingerprinting is used in a number of contexts including business and civil service. *See id.* at 1008. The court also stated that fingerprinting is required of all "employees of United States government agencies and departments." *Id.* Ultimately, the court held that the requirement did not invade the plaintiffs' right to privacy, nor did it violate a constitutional right. *See id.* at 1012.

116. *See id.* at 1008. *See also* Young v. Chicago Hous. Auth., 112 N.E.2d 719, 721 (Ill. App. Ct. 1953). The plaintiffs in *Young* brought suit against their employer, the Chicago Housing Authority. *Id.* The complaint was based on a mandatory fingerprinting policy which required all employees to undergo fingerprinting. *See id.* The prints were given to local law enforcement authorities for criminal matching. *See id.* Employment was partially based on whether the prospective employee had a criminal record. *See id.* The court held that no "stigma" is attached to fingerprinting anymore, and it is an accepted method of determining "employee fitness," and thus justified. *Id.*

117. *See* Kaplan, *supra* note 70, at 94. In addition to the use of fingerprints in the criminal context, fingerprints have been used in civil situations as well. *See id.* Fingerprinting is used in probate, hospitals, and in the identification of victims of train, air, and sea disasters. *See id.* Fingerprints have been used to substitute the signature of a testator or in conjunction with the testator's signature and are also used in hospitals for newborn identification. *See id.*

less offensive, because the process does not have the same characteristics of criminal fingerprinting.[118] Presently, fingerprinting is cleaner than the old criminal process.[119] The ink used to transcribe the fingerprint disappears when the fingers are rubbed together.[120] Furthermore, some banks use digital scanners, which do not use ink.[121]

The problem with looking at this process in a strict legal sense is that personal feelings are not considered. Regardless of whether the process violates a law or a plaintiff has a valid cause of action, fingerprinting still makes people feel as though they are not treated fairly. Ultimately, on-site fingerprinting may have an insulting effect on individuals, but the law does not offer a remedy for such a minor insult. Furthermore, the fact that customers voluntarily undergo fingerprinting makes their argument less compelling.

C. The Equal Protection Clause and On-Site Fingerprinting

Laws which operate to the disadvantage of a suspect class or inhibit the fundamental rights of citizens, will be subject to strict judicial scrutiny under the Fourteenth Amendment.[122] On-site fingerprinting raises a few discrimination issues, namely, whether a law which not only operates to the disadvantage of poverty stricken citizens is constitutional, but whether the poor, many of whom are minorities, are a suspect class, which would subject proposed legislation to strict judicial scrutiny; and whether this legislation would survive a strict scrutiny analysis. Generally, banks involved in on-site fingerprinting only require customers without accounts to provide a fingerprint. This may have a disproportionate effect on the poor.[123] An estimated twenty-five percent of U.S.

---

118. *See Finger Image Identification to Facilitate Electronic and Alternative-Channel Banking*, *supra* note 7. Modern fingerprinting is a clean and easy process which is not as intrusive as criminal fingerprinting. *See id.* Fingerprints are read by a scanner and then transformed into a binary code. *See id.* The unique characteristics of the print are extracted by the computer and a record of an individual's unique characteristics is stored. *See id.* The final step of the process is to compare the record against other records in the database. *See id.* This is done by the use of computer software which attempts to match the unique characteristics of the prints. *See id.*

119. *See id.*

120. *See* Sabatini, *supra* note 1, at D1. The great economic loss attributed to check fraud sparked a number of banks across the nation to adopt an inkless fingerprint program. *See id.*

121. *See* Sietz, *supra* note 64, at A1. There are two ways in which fingerprints are collected and stored. *See id.* The first is the traditional ink method. *See id.* The second method utilizes a digital scanner which reads the print, then stores it in a database for future matching. *See id.*

122. *See* San Antonio Indep. Sch. Dist. v. Rodriguez, 411 U.S. 1, 16 (1973).

123. *See* Kathy Hoke, *Banks, Attorney General Give Thumbs Up to Fingerprint Plan*, Bus. First of Columbus, Nov. 1, 1996, at 12. "Critics say the program raises questions about confidentiality and courtesy . . . . The vast majority of customers seek check cashing

households do not have bank accounts, and many of these households are in the lower income brackets.[124]

Many of these low income families are minorities. Although the proposed legislation does not discriminate on its face, it may operate to the disadvantage of many minorities. Only requiring non-account holders to undergo fingerprinting may have a disproportionate affect on minorities because they make up a large percentage of non-account holders. Subsequently, they will be forced to compromise their right to privacy, or to pay an inflated fee at a private check cashing business. It could be argued that this is unequal protection of the laws, thus a violation of the Fourteenth Amendment.

First, it is essential to determine whether the poor can be classified as a suspect class, thus invoking a strict judicial scrutiny analysis. In *San Antonio Independent School District v. Rodriguez*,[125] the constitutionality of the Texas school financing system was challenged.[126] The suit was brought on behalf of schoolchildren who were poor and residing in school districts with a low property tax base. Rodriguez argued that the poverty stricken students were discriminated against because of their families' economic status.[127] The basis of their claim was that students in school districts with low tax bases had lower per pupil expenditures than students in more affluent districts.[128] It was argued by Rodriguez that this low per pupil expenditure lessened the quality of the education the students received, thus depriving them equal protection of the law.[129]

One of the focal points of the case was to determine whether this class of poor individuals was a suspect class.[130] The district court held that the poor were a suspect class, then found the system unconstitutional under a strict scrutiny analysis.[131] That holding was overruled by the Supreme Court which concluded that the Texas system did not dis-

---

from banks are honest. An estimated twenty-five percent of U.S. households, predominantly poor, do not have checking accounts." *Id.*

124. *See id.*

125. San Antonio Indep. Sch. Dist. v. Rodriguez, 411 U.S. 1 (1973).

126. *Id.* at 4.

127. *See id.*

128. *See id.*

129. *See id.* at 16. The Edgewood School District, where the appellee's resided, had an assessed property value per pupil of $5,960 and a median family income of $4,686. *See id.* at 12. At an equalized tax rate of $1.05 per $100 of assessed property, the district contributed $26 for each child in the 1967-1968 school year. *See id.* In Alamo Heights, the assessed property value per pupil exceeded $49,000 with a median family income of $8,001. *See id.* at 13. In the same year that Edgewood supplied $26 per pupil under the Texas system, Alamo Heights supplied $333 per pupil. *See id.*

130. *See id.* at 19.

131. *See id.* at 6

criminate against any suspect class.[132] The basis for this conclusion was that the poor did not meet any of the "traditional indicia of suspectness."[133]

Like the poor in *San Antonio Independent School District*, the poor subjected to on-site fingerprinting would not fall into the category of a suspect class. The reasoning is virtually identical. Both systems, on-site fingerprinting and the Texas system, allegedly discriminate against a diverse "amorphous class." Both "classes" have only one common thread, poverty. In fact, the Supreme Court has never held that wealth per se is a suspect class.[134]

As mentioned earlier, the general policy of many banks is to subject all customers without accounts to the process. All customers, regardless of their race, national origin, gender, income, age, or sexual preference will be treated the same under the proposed law. However, even though a law may not mention any specific class, that does not mean that it does not discriminate. Laws which do not discriminate on their face may still be subject to a strict scrutiny analysis. In addition to proving that the law discriminates against a suspect class, motive must also be proven before the law is subject to strict scrutiny.[135]

Implementing a law which gives banks the option of conducting on-site fingerprinting serves a number of state interests, namely, limiting criminal activity.[136] Furthermore, using on-site fingerprinting is not the only method of limiting criminal activity in this field, but it is the most reasonable. There are other ways to reduce check fraud. The use of picture identification such as a driver's license is one method. However, this method poses a number of problems. First, not every citizen has a driver's license. Second, criminals have access to highly sophisticated equipment which enable them to create fraudulent checks, and there is nothing stopping the same criminals from creating fraudulent drivers' licenses.[137]

On-site fingerprinting eliminates both problems. The person's identity will be fixed to the back of the check or filed in a database. Regardless of whether the check or the license is fraudulent, the fingerprint is an unmistakable piece of identification which directly links the criminal to scene of the crime. A criminal conviction based purely on fingerprint

132. *Id.* at 28.

133. *Id.* Traditional indicia of suspectness include: "a history of purposeful and unequal treatment, or relegated to such a position of political powerlessness as to command extraordinary protection from the majoritarian political process." *Id.*

134. *See id.*

135. *See* Washington v. Davis, 426 U.S. 229, 240 (1976).

136. *See* Stammen, *supra* note 3, at C6.

137. *See* Sabatini, *supra* note 1, at D1.

evidence can be sustained.[138] Furthermore, testimony of a teller or video surveillance which places the criminal at the scene will strengthen the state's case.

Aside from the constitutional issues, on-site fingerprinting may have a stigmatizing effect upon the less fortunate, because they may not have the option of going to a different institution.[139] Under New York law, welfare recipients are required to undergo fingerprinting[140] and critics of this system argue that this stigmatizes the poor.[141] The system requires

---

138. *See* People v. Rhodes, 422 N.E.2d 605, 608 (Ill. 1981).

> Fingerprint evidence is circumstantial evidence which attempts to connect the defendant to the offense alleged. In order to sustain a conviction solely on fingerprint evidence, fingerprints corresponding to fingerprints of the defendant must have been found in the immediate vicinity of the crime under such circumstances as to establish beyond a reasonable doubt that the fingerprints were impressed at the time the crime was committed.

Id. (citation omitted).

139. *See* Constance, *supra* note 9, at 403. Recently, New York, as well as many other states, have implemented "automated fingerprint identification" systems into their welfare programs. *See id.* This program was created to reduce welfare fraud. *See id.* A recipient's fingerprint is read by a scanner and then logged into a database. *See id.* at 401. When a recipient applies for welfare assistance, his or her print is scanned, and then matched against fingerprints in the database. *See id.* A welfare applicant does not have the options of choosing a different institution, so they are "forced to submit to an unjustifiable degree of intrusion." *Id.* at 403.

140. *See* N.Y. SOCIAL SERVICE LAW Sec. 139-a (McKinney 1997).

Special provisions to avoid abuse of assistance and care

> 3. (a) The social services districts of Allegheny, Broome, Dutchess, Niagara, Onondaga, Oneida, Orange, Oswego, Rensselear, Rockland, Steuban and Suffolk shall authorize and implement demonstration projects for the purposes of determining the cost effectiveness of preventing multiple enrollment of home relief benefit recipients through the use of an automated two digit finger imaging matching identification system. The system shall only include home relief benefit recipient finger imagining upon application of eligibility for such benefits and finger imaging of home relief recipients currently receiving home relief benefits.
>
> (b) Notwithstanding the provisions of section one hundred thirty-six of this article or any other provision of law, data collected and maintained through the use of an automated finger imaging matching identification system as authorized by this subdivision may not be used, disclosed or redisclosed for any purpose other than the prevention of multiple enrollments in home relief, may not be used or admitted in any criminal or civil investigation, prosecution or proceeding, other than a civil proceeding pursuant to section one hundred forty five-c of this article, and may not be disclosed in response to a subpoena or other compulsory legal process or warrant, or upon request or order of any agency, authority, division, office or other private or public entity or person, except that nothing contained herein shall prohibit disclosure in response to a subpoena issued by or on behalf of the applicant or recipient who is the subject of the record maintained as part of such system. Any person who knowingly makes or obtains any unauthorized disclosure of data collected and maintained through the use of an automated two-digit finger imaging matching identification system shall be guilty of a class A misdemeanor, and shall be punished in accordance with the provisions of the penal law.

Id.

141. *See* Constance, *supra* note 9, at 406.

the poor to submit to a process that makes them feel like they are being arrested.[142] It is argued that this process "vilifies" the "outcast status" of the less fortunate.[143]

However, when applied to the banking industry, the "stigmatizing effect" argument is invalid. The primary reason is because banks require that all non-account holders undergo fingerprinting, regardless of their income level. Often, those who are turned away are not poor, they just refuse to be fingerprinted. Furthermore, unlike welfare recipients, bank customers have other options as checks can be cashed at a number of locations.

D. Accumulation of Personal Information

The buying and selling of personal information is something citizens should keep in mind. The accumulation of small violations may add up to become a vast amount of information.[144] Furthermore, technology has made this information accessible to almost anyone.[145] It seems as though "Big Brother" is once again acquiring yet another piece of information.[146]

Consumers should also be concerned with who may have access to their prints. On-site fingerprinting gives the bank direct access to customers fingerprints. These fingerprints are kept on file until fraud occurs.[147] However, checks are typically sent back to the provider upon

142. *See id.*

143. *See id.*

144. *See* Eric Grossman, *Conceptualizing National Identification: Informational Privacy Rights Protected,* 19 J. Marshall L. Rev. 1107, 1010 (1986). In 1983, it was estimated that the government had approximately four billion records of information on individuals. *See id.*

145. *See* Ellen Alderman & Caroline Kennedy, The Right To Privacy 323 (1995). People have been providing personal information to a number of sources. *See id.* For example, citizens give personal information to credit bureaus, credit card companies, the IRS, banks, and insurance companies. *See id.* However, this information was generally kept secretive, and placed in files. *See id.* But since the advent of the computer and the information superhighway, this information can be accessed by a great number of individuals. *See id.* The FBI discovered a group of "infobrokers" who obtained and sold information which was stored in government files. *See id.* at 325. An alarming example depicting the ease in accessing personal information is when a journalist having a computer, a phone and fifty dollars obtained the Vice President's credit report. *See id.* Much of this information can be obtained legally as well. *See id.* For example, until recently, driving records were public information. *See id.* A person merely has to pay a fee and he can access a person's driving history. *See id.* Also, the post office passes personal information onto marketers for a fee and these marketers may freely sell this information. *See id.*

146. *See* George Orwell, 1984 (1949). The crux of Orwell's fictional story addressed how privacy rights may deteriorate with the onset of technological advancements. *See id.*

147. *See* Mary Fricker, *Putting a Finger On Fraud Banks Begin Requiring Prints to Cash a Check,* Press Democrat (Santa Rosa, Cal.), March 30, 1997, at E1. After the customer puts their print on the check, it is processed like all other checks. *See id.* Eventually

cashing or depositing.[148] Therefore, the entity that provided the consumer with the check will also have the consumer's print. There is no guarantee that they will not sell or give the prints away. However, some critics have questioned what a person could do with a print.[149] Although they may not be of any use now, future technology may provide them with capacity to access bank accounts, or perhaps fraudulently cash checks.

It is the banking industry's policy not to disclose customer information to anyone. However, there are a number of exceptions to this rule. For example, banks will disclose information regarding a customer's account when fraud is suspected. Fingerprints would fall under this exception and in fact, this is one of the primary reasons for having an on-site fingerprinting policy. Potential criminals who know that their fingerprints will be provided to law enforcement officials would certainly reconsider violating the law.

There are alternative information systems that have been in use for years. For example, "Electronic Fund Transfers" have been in use and have been quite successful for a number of years. Common examples of electronic fund transfers systems are Automated Teller Systems, Point of Sale Systems, and Check Guarantor Systems.[150] The Point of Sale system checks the status of the customer's account and determines whether the customer is credit worthy. If the determination is in the affirmative, the check will be cashed.

Another system is a service which lists customers with bad check status.[151] This list is provided by a service which charges customers a fee. In recent years, the service has been implemented into the Internet, making the information readily accessible. The problem with the service being on-line is that it is readily accessible, and this private information is available to anyone who is willing to pay a fee.

E. Public Reaction to On-site Fingerprinting

There have been mixed emotions relating to consumer acceptance of

---

the check is either stored in the bank or it is returned to the writer. *See id.* This is the normal procedure, unless it turns out that the check is fraudulent. *See id.* If the check is fraudulent, it is then immediately turned over to the FBI as evidence of the crime. *See id.*

148. *See id.*

149. *See* Uri Berliner, *Thumb's Down Banks' Growing Use of Fingerprints Riles Advocates of Privacy*, San Diego Union-Trib., March 13, 1997, at C1. A representative of Identicator Corp., a fingerprint equipment supplier to many banks, stated that fingerprints are useless to anyone outside the field of law enforcement because fingerprints are only useful to those with access to a search engine. *See id.*

150. George B. Trubow, Privacy Law and Practice § 3.01 (1991).

151. *See id.* at § 3.01(5)

on-site fingerprinting.[152] Although people understand why the banks are using on-site fingerprinting, some individuals refuse to accept it.[153] For instance, police in Florida have been called in to remove "riled" consumers who were not pleased with the new program.[154]

As of now there is no law which prohibits banks from requiring fingerprints. But based on public reaction to fingerprinting, and the personal experience of some legislative members, new bills have been proposed to thwart some fingerprinting processes.[155] For example, there is a pending bill in the Georgia House of Representatives which, if passed, would prohibit banks from requiring fingerprints for check cashing.[156] The Georgia bill requires banks to honor the checks of non-ac-

152. *See Finger Image Identification to Facilitate Electronic and Alternative-Channel Banking, supra* note 7. Seventy-seven percent of those polled believe that requiring a fingerprint for the cashing of a large check is justified. *See id.*

153. *See Banking Fees, Thumbprinting Cause Outcry*, FLORIDA TODAY, Dec. 27, 1996, at 10C. The new check cashing polices of a number of Florida banks are unpopular with the Floridians. *See id.* The tempers of many Floridians have risen when they were asked to undergo fingerprinting as part of new bank policies. *See id.* Some banks had to call in the police to remove disgruntled customers. *See id.*

154. *Id.*

155. *See* Sandra Eckstein, *Legislature '97 New Bills Target Consumer Issues Fingerprinting, Telemarketing on List,* ATLANTA J. CONST., Jan. 23, 1997, at A4. A number of new proposals have caught the attention of the Georgia House of Representatives. *See id.* Among the hottest topics was the questionable practice of requiring fingerprints to cash checks or to receive drivers licenses. *See id.* Representative Roy E. Barnes (D-Mableton) sponsored a bill and co-sponsored another which if passed would prohibit fingerprinting for such purposes as check cashing and drivers licenses. *See id.*; Kulman, *Bank Thumbprinting Shameful Invasion of Privacy,* ASHBURY PARK PRESS, June 6, 1997, at A21. Assemblywoman Nia Gill, (D-Essex) sponsored bills that discouraged banks from fingerprinting by prohibiting the state from doing business with financial institutions that required fingerprints. *See id.* State Senator Wynona Lipman, (D-Essex) introduced a bill with similar ramifications. *See id.*; *See* Sam Ali, *Check Payees Give Thumbs Down to Fingerprinting by First Union*, STAR LEDGER (Newark, N.J.), Apr. 11, 1997. Two "Democratic lawmakers" introduced bills in the Georgia House of Representatives that would make it illegal for banks to require fingerprinting for check cashing. *Id.* The bills would also prohibit the state and its agencies from conducting business with banks that require fingerprints. *See id.*

156. *See* H.R. 33, 94th Leg., 1st Reg. Sess. (Ga. 1997). This Bill states in pertinent part:

> To amend Part 1 of Article 2 of Chapter 1 of Title 7 of the Official Code of Georgia Annotated, relating to general matters applicable to banks and trust companies, so as to provide that no such institution shall require a fingerprint as a requirement for cashing a check or similar instrument; to provide that a financial institution shall cash certain checks on which the state is maker; to provide an effective date; to repeal conflicting laws; and for other purposes.
>
> SECTION 1.
>
> Part 1 of Article 2 of Chapter 1 of Title 7 of the Official Code of Georgia Annotated, relating to general matters applicable to banks and trust companies, is amended by inserting at the end thereof the following:
>
> 7-1-245.

count holders without taking fingerprints.[157]

F. The Benefits of On-site Fingerprinting

This minor invasion of privacy poses a great benefit to society.[158] Some legal scholars argue that some invasions of privacy are not significant enough to warrant protection of the laws.[159] Warren and Brandeis stated that when determining the intrusiveness of an invasion, the privacy rights should be weighed against the benefits society yields from the invasion.[160] Obviously, reducing criminal acts and reducing the ten billion dollars per year loss in revenue to the banking industry is of paramount importance to society.[161]

Reduction in check fraud would mean more profit for the banking industry, which would yield better rates for consumers. Furthermore, fewer cases of fraud would improve the government's fight against check fraud.[162] Moreover, law enforcement agencies would have the criminal's fingerprint, making identification of criminals easier.[163]

In addition, fingerprinting is an excellent tool for security purposes, and it has become widely accepted in our society. As mentioned earlier, many institutions require fingerprints for drivers licenses, memberships, and employment, which has essentially lessened its association with

---

> No financial institution subject to the provisions of this article shall require a person to provide a fingerprint in any form as a requirement for cashing a check or similar instrument.

Id.

157. *See id.*

158. *See* Thao Hua, *Fingerprinting Hailed in the Fight Against Fraud,* L.A. Times, May 25, 1997. Hundreds of banks in the state of California require that customers give their fingerprints when they want to cash a check. *See id.* In addition to the banking industry, many other businesses have the same requirements. *See id.* Although a number of people disagree with the program, "[l]aw enforcement officials are hailing the system as a weapon against check fraud that surpasses even the drivers licenses, which in the age of computers has become a cinch to counterfeit." *Id.* Many arrest have resulted from the fingerprinting process, and Anaheim police have stated that they have identified the signers of at least "80% of forged, fingerprinted checks, resulting in about 10 convictions" *Id.*

159. *See* Warren & Brandeis, *supra* note 14, at 214.

160. *See id.* "To determine in advance of experience the exact line at which the dignity and convenience of the individual must yield demands of public welfare or of private justice would be a difficult task . . . " *Id.* Warren and Brandeis also state that the right to privacy does not "prohibit the publication of matter which is of public or general interest." *Id.*

161. *See* Sabatini, *supra* note 1, at D1. It is estimated by the Federal Reserve that losses from check fraud account for nearly $10 billion annually. *See id.*

162. *See Finger Image Identification to Facilitate Electronic and Alternative-Channel Banking, supra* note 7. Finger imaging is not as invasive as the traditional methods of fingerprinting, but the public must "overcome" the association of fingerprinting with criminal activity. *Id.*

163. *See* Hua, *supra* note 153.

criminal activity.[164]

IV. CONCLUSION

The new policy imposed by the banking industry does not invade privacy rights protected by the First, Third, Fourth, Ninth, or Fourteenth Amendments. Nor does the process of on-site fingerprinting invade personal privacy protected by common law doctrines. Finally, the process does not violate the equal protection clause or the due process clause of the Fourteenth Amendment.

The United States Supreme Court has never held that fingerprinting per se invades privacy rights protected by the Constitution.[165] Fingerprinting is only a slight inconvenience, and does not involve any of the probing into one's life or thoughts protected by the Constitution.[166] Furthermore, the impact of fingerprinting on one's dignity is minimal, leaving those offended by the process with no legal solution. The strength of the argument against on-site fingerprinting is weakened by the fact that fingerprinting is used for a variety of civil purposes[167] and the use of inkless dyes and digital scanners have changed the fingerprinting process so much that it no longer resembles a criminal fingerprinting.

Assuming that on-site fingerprinting invades the fundamental right to privacy, it is nevertheless justified upon a showing of a compelling state interest.[168] Fingerprinting is a security measure implemented in order to reduce crime, which accounts for a ten billion dollar per year loss to the banking industry.[169] It is certainly a compelling state interest to reduce criminal activity and curb this tremendous loss.

In addition, anything an individual knowingly exposes to the public does not warrant the protection of constitutional privacy rights.[170] People literally leave their prints on everything they touch.[171] Regardless of

164. *See* United States v. Kelly, 55 F.2d 67, 70 (2d Cir. 1932). "Fingerprinting is used in numerous branches of business and of civil service, and is not in itself a badge of crime." *Id.* Thom v. New York Stock Exch., 306 F. Supp. 1002, 1007 (S.D.N.Y. 1969). ("To the same effect is a state court's contemporaneous opinion upholding a regulation requiring fingerprinting for the issuance of a license to deal in secondhand articles.").

165. *See* Davis v. Mississippi, 344 U.S. 721, 727 (1969).

166. *See id.*

167. *See Thom,* 306 F. Supp. at 1008; Kaplan, *supra* note 70, at 94.

168. *See Thom*, 306 F. Supp. at 1007.

169. *See* Sabatini, *supra* note 1, at D1.

170. *See* Katz v. United States, 389 U.S. 347, 351 (1967). Anything knowingly exposed to the public does is not subject to the protection of the Constitution's Fourth Amendment. *See id.*

171. *See* O'HARA & O'HARA, *supra* note 108, at 682. The fingerprints of an individual are transferred to an object by merely touching it. *See id.* Although the print is most likely present, it may be difficult to see based on the material touched. *See id.* For example,

whether anyone can see them or not, they are still made public.[172] Knowingly exposing fingerprints to society will certainly reduce a persons expectation of privacy associated with their fingerprints.

Although this process may make some people feel violated or uncomfortable, the law offers no remedy. Individuals must learn to become callous to these minor invasions. It would be entirely unreasonable to afford a legal remedy to all intrusions, no matter how slight. If this were not the case then every incidental bump on the train or obscene gesture on the street would draw the attention of the courts.

Patrick J. Waltz

fingerprints are most visible on hard glossy surfaces as opposed to soft, absorbent surfaces. *See id.*

172. *See id.*