UIC John Marshall Journal of Information Technology & Privacy Law

Volume 23
Issue 2 *Journal of Computer & Information Law - Winter 2005*

Article 5

Winter 2005

Age Verification in the 21st Century: Swiping Away Your Privacy, 23 J. Marshall J. Computer & Info. L. 363 (2005)

John T. Cross

COMMENTS

AGE VERIFICATION IN THE 21ST CENTURY: SWIPING AWAY YOUR PRIVACY

I. INTRODUCTION

After a long hard workweek, on Friday evening you decide to meet up with a few friends at a neighborhood bar near your home. On your way to the bar, you stop by a convenience store to purchase a pack of cigarettes. You walk in the door and tell the man working behind the counter what you want. He grabs the cigarettes and asks you for identification to assure you are over the age of eighteen. He then takes your driver's license and swipes it through a scanning device. This device reads the information encoded in the barcode on the back of your driver's license to determine if the license is valid and verifies your age. The light on the device turns green, and he proceeds to sell you the cigarettes.

You continue down the street to the neighborhood bar, your original destination. Once there you are greeted by the doorman, who asks you for your identification to assure you are of legal age. You again hand over your driver's license, and he swipes it through a scanning device. The device once again reads the barcode on the back of your license, the light turns green, and he hands the license back to you and allows you to enter. You enter the bar, without thinking anything has just happened to you besides your age being checked to assure that you are old enough to purchase cigarettes or consume alcohol, and enjoy the evening with some friends.

This whole scenario may sound like an excerpt out of a futuristic science fiction novel, but the practice of driver's license swiping is occurring at many types of private businesses where proof of age or security issues arise.[1] This practice of "swiping" has beneficial uses for both pri-

1. Rina C.Y. Chung, *Hong Kong's "Smart" Identity Card: Data Privacy Issues and Implications for a Post-September 11th America*, 4 U. of Haw. Asian-P. L. & Policy J. 442, 443 (2003); Jennifer Lee, *Welcome to the Database Lounge*, N.Y. Times G3 (Mar. 21, 2002); Kim Zetter, *Great Taste, Less Privacy*, http://www.wired.com/news/print/0,1294,62182,00.html (last updated Feb. 6, 2004); Deborah Pierce, *Swiping driver's licenses – instant marketing lists?*, http://www.seattlepress.com/print-10148.html (last updated Mar. 31, 2003).

vate entities, in identifying underage persons and those with fake identification,[2] and law enforcement.[3] However, the problem is that in the private sector, businesses are not using the information to merely identify underage customers or those with fake identification; many are storing the information encoded on the barcode in a computer database.[4] Currently, no federal laws and very few state laws regulate the collection and use of this information.[5] Basic guidelines exist to make people aware that their information is being collected electronically and to alert them to how it is being used.[6] Yet, the private sector is not following these guidelines.[7]

The information is stored on drivers' licenses electronically via either a magnetic strip or a barcode, and is obtained by swiping a license through a scanning device.[8] The data encoded ranges from basic name, address, and expiration date information to much more intrusive information such as social security number, electronic fingerprint, and electronic image of the holder's signature.[9] Some states encrypt data that is more sensitive, like electronic fingerprints or photographs, so only law enforcement officials can decode it, but others do not.[10] There are also guidelines set forth for the collection of electronic data, the Fair Information Practice Principles, which are supposed to protect people by informing them that their data is being collected and how it is used.[11] However, without some type of enforcement, these guidelines are just guidelines.[12] Currently, there is no type of redress against private entities for people whose information is not collected according to the

2. Nicole Christiansen, *Machines detect fake IDs*, LXXXVII The Aquin 3 (Sept. 27, 2002) (available at http://www.stthomas.edu/aquin/092702/00092702.pdf).

3. *Great Taste, Less Privacy*, *supra* n. 1 at [¶ 10], http://www.wired.com/news/print/0,1294,62182,00.html.

4. Chung, *supra* n. 1, at 443.

5. *Id.*

6. Fed. Trade Commn., *Privacy Online: A Report to Congress*, at III (June 1998) (accessible online at http://www.ftc.gov/reports/privacy3/toc.htm.) [hereinafter *FTC Report*].

7. *See generally* Swipe, *Research*, http://www.we-swipe.us/research.html (last accessed Nov. 18, 2004) (stating that usually businesses do not ask for consent before swiping a person's license, or even notify the person that the swiping has taken place).

8. *Great Taste, Less Privacy*, *supra* n. 1, at [¶¶ 1-5], http://www.wired.com/news/print/0,1294,62182,00.html.

9. Chung, *supra* n. 1, at 443; *Research*, *supra* n. 7 at *What Information is Encoded on Drivers' Licenses?*.

10. Cal. Assembly Comm. on Jud., A.B. 224 *Privacy: Electronic Reading and Use of Identification Card Data*, 2003-2004, at 3 (Mar. 4, 2003); *Infra* nn. 265-266 (discussing that most states encode biometric data so that only law enforcement can access it, and discussing the precautions Illinois takes to protect encoded data) [hereinafter *Electronic Reading*].

11. *FTC Report*, *supra* n. 6; *infra* pt. II(D) (giving a brief history of and setting forth a brief description of the fair information practice principles).

12. *Id.* at III(5).

principles.[13]

Law enforcement officers,[14] as well as private businesses, have the ability to use the information in several ways.[15] First law enforcement officers are able to make their work more efficient and safe.[16] They can scan the license to instantly complete data fields of electronic citations, and to run up to the minute background checks on people they have stopped.[17] Furthermore, police may call private establishments that scan and retain data to determine if a certain person has visited the business recently,[18] or to obtain personal records from the enterprise about an individual.[19]

Private entities may use the scanning and information retention for their own benefits as well.[20] The most obvious benefit is the reduction in underage drinking and smoking because the entities can easily tell the age of the patron, and identify fraudulent identification.[21] Through the stored data, an establishment can also learn a great deal about its customer base, and then directly market entertainment events and promotions to specified individuals it believes would be most interested in the event.[22] A business may also program a scanner to reject a certain individual because that person has caused problems at the enterprise in the past.[23] This information helps protect the safety of patrons.[24]

The problem arises not with business enterprises scanning the licenses, but with the storage of the data obtained through the swipe. The private sector intends to use scanning and data storage only for age ver-

13. *Research*, *supra* n. 7, at *Commercial Data Warehouses*.

14. *Great Taste, Less Privacy*, *supra* n. 1, at [¶12], http://www.wired.com/news/print/0,1294,62182,00.html.

15. *See* Christiansen, *supra* n. 2.

16. *See generally* Zebra Technologies, *Electronic Citation Systems: The Safe Choice to Save Time and Improve Accuracy* (Jan. 2004) (available at http://www.zebra.com/whitepapers/WP13503Lcitation Sys.pdf) (noting how law enforcement officers can make their jobs safer by swiping because they can get immediate information and keep their attention focused on the suspect) [hereinafter *Electronic Citation Systems*]; Bob Howie, *Oak* Ridge *to update court software; Old system slows processing of information*, The Houston Chronicle Sec. This Week Pg. 3, [¶ 6-9] (June 24, 2004); *Great Taste, Less Privacy*, *supra* n. 1, at [¶ 12], http://www.wired.com/news/print/0,1294,62182,00.html.

17. *Electronic Citation Systems*, *supra* n. 16.

18. *Great Taste, Less Privacy*, *supra* n. 1, at [¶ 15], http://www.wired.com/news/print/0,1294,62182,00.html.

19. *See generally* Lee, *supra* n. 1, at [¶ 15].

20. Chung, *supra* n. 1, at 443; Lee, *supra* n. 1; *Great Taste, Less Privacy*, *supra* n. 1, http://www.wired.com/news/print/0,1294,62182,00.html; Christiansen, *supra* n. 2.

21. Chung, *supra* n. 1 at 443.

22. Lee, *supra* n. 1 at [¶¶ 22-27].

23. *Id.* at [¶ 31].

24. *See Id.* at [¶ 31] (noting how easily a bar or restaurant can program a scanning device to reject a troublesome person's admittance, and implicitly stating how all patron's safety increases by preventing troublesome patrons into the establishment).

ification and marketing purposes,[25] but the possibility of the information falling into the wrong person's possession abounds.[26] If an individual at the business collecting the data personally possessed the records, the possibility of crimes such as stalking and identity theft are possible, not to mention more severe crimes like rape or murder.[27] Such sensitive data should be protected from falling into the wrong person's possession through some type of regulation or legislation.

Several states have acted on the subject and have developed laws prohibiting the use of swiping.[28] Some states also regulate the amount of information that can be obtained and the purposes for which it may be stored.[29] However, in most states, the practice is entirely unregulated.[30] Most people either have no idea that the transfer and storage of data occurs, or do not know the amount of information being conveyed and saved.[31]

This comment seeks to argue that United States citizens have a right to privacy with regard to the information contained on their identification cards.[32] First, the background of the comment will describe how swiping technology works and what types of regulations currently exist to govern swiping. This section will also introduce the Fair Information Practice Principles, and give a brief history of their application. The

25. Chung, *supra* n. 1 at 443 ("Furthermore, the bar's management may decide to collect this information and use it to build up its own customer database for marketing purposes").

26. *Great Taste, Less Privacy*, *supra* n. 1, at [¶ 23], http://www.wired.com/news/print/0,1294,62182,00.html (A bar employee could use the database to make a list for stalking purposes of " all blond female patrons between the ages of 21 to 25 who weigh 120 pounds." The scanners bars and restaurants use are handheld so "an employee could pull out a personal scanner and scan cards twice to sell the data for ID theft crimes").

27. *Id.* at [¶¶ 23-24], http://www.wired.com/news/print/0,1294,62182,00.html.

28. *Research*, *supra* n. 7, at *Is Swiping Happening in my State?*.

29. *Id.*

30. Chung, *supra* n. 1 at 443; *Infra* II(C)(i)-(v) (discussing which states have regulations limiting the use of swiping and subsequent data retention by private businesses).

31. *Great Taste, Less Privacy*, *supra* n. 1, at [¶¶ 1-6], http://www.wired.com/news/print/0,1294,62182,00.html.

32. U.S. Const. amend. I ("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 to petition the Government for a redress of grievances."); U.S. Const. amend. IV; ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated. . ."); *see Roe v. Wade*, 410 U.S. 113, 152 (1973) (stating that even though the Constitution does not explicitly state a right to privacy, the Supreme Court of the United States has often recognized a right to personal privacy); *See* Don Goldhamer, *Privacy Concerns*, Swiss House for Advanced Research and Education Presentation, Boston Mass. (July 24, 2000) (available at http://home. uchicago.edu/~dhgo/privacy-intro/index. html) (describing American's general rights to privacy and how the Constitution and Supreme Court interpret them).

comment then discusses all the current applications of swiping, including law enforcement and private enterprise use. The potential costs and benefits of scanning and data retention are analyzed to determine whether the practice should continue to be unregulated in private enterprises. The comment will argue that a person should have the right to purchase something that is legal without having to exchange his or her sensitive information for this item. People should also be aware that their information is being collected and receive notice as to how it could be used.[33] Lastly, this comment suggests that legislation be put in place to regulate the practice of scanning and storing patron's personal information. As the practice of swiping becomes widespread among private enterprises that must check for proof of age,[34] inevitably, this information may fall into the wrong person's hands and this must be prevented from happening.

II. BACKGROUND

The practice of swiping identification to verify age is rather new. Only with the advent of a majority of states having encoded data on their drivers' licenses via a magnetic strip or two-dimensional barcode was the practice feasible. Currently over forty states store encoded data on their licenses, and most of the rest of the states are planning to do so in the near future.[35] The widespread use of licenses containing encoded data, coupled with the proliferation of private businesses purchasing and using scanning equipment to swipe the cards, has placed the issue on center stage.[36] Demonstratively, there is federal law prohibiting departments of motor vehicles from releasing an individual's information to a private entity.[37] However, there is no federal law, and very few state

33. *See FTC Report*, *supra* n. 6, at III (noting that people often have their personal information collected without their knowledge and that some type of legislation should be enacted to alert people this practice is taking place).

34. Chung, *supra* n. 1 at 443 ("In the United States a growing number of private businesses are utilizing this driver's license scanning technology. Bars and convenience stores increasingly rely on this technology to avoid illegal sales of alcohol and cigarettes to underage purchasers").

35. Lee, *supra* n. 1, at [¶ 7] ("Already, about 40 states issue driver's licenses with bar codes or magnetic stripes that carry standardized data, and most of the others plan to issue them within the next few years"); *infra* n. 78 (discussing that the only states which currently do not use some type of electric data encryption on their licenses are Alaska, New Jersey, and Wyoming).

36. *See generally* Lee, *supra* n. 1 (addressing the fact that many private businesses are either swiping currently, or will be in the near future); *Research*, *supra* n. 7 (noting numerous issues that have arisen solely from swiping.

37. Lee, *supra* n. 1 at [¶¶ 16-19] (Congress passed the Driver's Privacy Protection Act in 1994 "to limit the amount of information that can be released by departments of motor vehicles").

laws preventing a private entity from collecting the information directly from the individual.[38]

A. License Data

In the past, drivers licenses in all states only contained a limited amount of data displayed on the front of the license.[39] The information was basic and included items such as name, address, date of birth, and possibly social security number.[40] In order to retrieve any information off the license, the reader simply read the data from the license.[41] Over the last decade or so drivers' licenses that are machine-readable have come into existence.[42] The new license contains a magnetic strip or two dimensional barcode with data encoded on it.[43] Now instead of having to manually read or write down the information in order to store it, the license is swiped through a digital scanner and the data encoded on the strip is transferred to a computer.[44]

Originally, the new licenses had the same data encoded on them as what was printed on the front.[45] Swiping the license could attain the data faster, but the person scanning it could not access any more data than what the license contained in print format. With the advent of better technology though, the data encoded on the license is now in greater detail, and much more private than what is printed on the front.[46] A number of licenses now include information in addition to the basic information.[47] For example, Kentucky embeds a digital picture of the holder on the barcode of its licenses.[48] Washington D.C., Georgia, and Hawaii all include digital fingerprints on their barcodes, and Tennessee includes

38. *Id.* at [¶ 19] (". . . there are only spotty controls over how businesses can create such databases on their own."); *Research*, *supra* n. 7, at Is Swiping Happening in my State? ("It is also a state choice to regulate driver's license swiping or—in more instances—not regulate.").

39. Lee, *supra* n. 1 at [¶¶ 14-16].

40. *Id.*

41. *See Id.* (describing alternate ways of retrieving information off of drivers' licenses other than swiping).

42. *Id.* at [¶¶ 6-8].

43. *Great Taste, Less Privacy*, *supra* n. 1, at [¶ 4], http://www.wired.com/news/print/0,1294,62182,00.html.

44. *See Id.* at [¶ 17] (describing how easily data collection has become through swiping).

45. Lee, *supra* n. 1 at [¶¶ 14-16].

46. *Research*, *supra* n. 7, at *What Information is Encoded on Drivers' Licenses?*.

47. *Id.*; *Great Taste, Less Privacy*, *supra* n. 1, at [¶ 11], http://www.wired.com/news/print/0,1294,62182,00.html.

48. *Great Taste, Less Privacy*, *supra* n. 1, at [¶ 11], http://www.wired.com/news/print/0,1294,62182,00.html; *Research*, *supra* n. 7, at *What Information is Encoded on Drivers' Licenses?*.

a facial recognition template.[49] Information encrypted in other states includes digital signature, social security number, and medical indicators.[50]

The information is actually stored on the back of the driver's license in either a magnetic strip or a two dimensional barcode.[51] The magnetic strip licenses have a solid dark stripe across the top of the back of the license.[52] A machine places magnetic fields of data on the strip that usually includes the data printed on the front of the license.[53] A magnetic strip scanner is needed in order to retrieve the encoded data from the license, and software is needed in order to translate the data into readable information.[54] Magnetic strips cannot hold near as much information as a two dimensional barcode, and have no security or encryption capabilities.[55] Therefore, no biometric information such as digital photos, fingerprints, or signatures can be stored on magnetic strips.[56]

The two dimensional barcode is a more advanced tool for encoding data on the back of licenses, and currently more than thirty states use it.[57] The two dimensional barcode is a series of ink printed bars on the back of a driver's license.[58] It looks different from a traditional barcode used on grocery packaging because it has the second dimension that enables storage of greater amounts of data.[59] It may be two square inches or larger, and traditionally replaces the magnetic strip.[60] Since the two-dimensional bar code can store much more data than a magnetic strip, it is capable of storing compressed data in various forms including photos, digital fingerprints, or digital signatures.[61]

The information from a two dimensional barcode is retrieved in a very similar fashion as the magnetic stripe.[62] A scanner is required to read the barcode, and software is required to translate the data into a

---

49. *Research*, *supra* n. 7, at *What Information is Encoded on Drivers' Licenses?*.

50. *Id.*

51. *Id.* at *How do* ID *Card Technologies Work?*; *Great Taste, Less Privacy*, *supra* n. 1, at [¶ 4], http://www.wired.com/news/print/0,1294,62182,00.html.

52. Positive Access Corporation, *Frequently Asked Question (FAQ)*, http://www.positiveaccess.com/faqs.html (last updated Aug. 27, 2004).

53. *Id.*

54. *Id.*

55. *Research*, *supra* n. 7, at *How do* ID *Card Technologies Work?*.

56. *See Id.* (stating that magnetic strips cannot hold as much information as two dimensional barcodes, and that unlike the magnetic strip data can be encrypted on the two dimensional barcode).

57. *Frequently Asked Questions*, *supra* n. 52; *Infra* n. 79 (discussing that thirty-nine states currently use two-dimensional barcodes to encrypt data on their drivers' licenses).

58. *Frequently Asked Questions*, *supra* n. 52.

59. *Id.*

60. *Id.*

61. *Id.*

62. *Id.*

readable form.[63] Unlike on a magnetic strip, the compressed data encoded on two-dimensional bar codes is supposed to be encrypted by the state to limit its access to law enforcement agencies only.[64] The technology is available to encode and include all types of information on new driver's licenses, but the legislation to regulate what can be done with that data has lagged far behind.

B. Federal Laws

1. *Drivers Privacy Protection Act ("DPPA")*

The DPPA is a federal law passed in 1994 in response to various crimes committed by people who obtained information about their victims from the Department of Motor Vehicles ("DMV").[65] The most prominent example was the 1989 murder of actress Rebecca Schaeffer, who was killed by an obsessed fan that obtained her address from the California motor vehicle record.[66] Another crime took place in Iowa during the same time and in a similar manner.[67] A band of thieves obtained their victims' addresses by writing down the license plate number of expensive cars and then obtaining the home address information from the department of motor vehicles.[68] Consequently, Congress enacted the DPPA to stop such abuses of the department of motor vehicles.[69] Before the DPPA was enacted, obtaining a person's private information for the purpose of committing crimes was far too easy.[70]

The DPPA prohibits a state department of motor vehicles from disseminating the information contained on a persons motor vehicle record.[71] The statute prevents the release of both "personal information"[72]

---

63. *Frequently Asked Questions*, *supra* n. 52.

64. *Id.*

65. Electronic Privacy Information Center, *The Drivers Privacy Protection Act (DPPA) and the Privacy of Your State Motor Vehicle Record*, http://www.epic.org/privacy/dppa/default.html (last updated Aug. 14, 2004) [hereinafter *DPPA and Privacy*].

66. *Id.* (Rebecca Schaefer was an actress and California resident. In 1989, an obsessed fan hired a private investigator to obtain Ms. Schaefer's address. The investigator did so through the California motor vehicle record. The fan subsequently stalked and killed Ms. Schaefer. When passed, the DPPA contained many exceptions, or reasons that a driver's motor vehicle record may be legally used. Included in that list of exceptions is the use by a licensed investigator or security service (18 U.S.C. § 2721(b)(7) (2000)), the very means Ms. Schaefer's murderer used to retrieve the address).

67. *Id.*

68. *Id.*

69. *Id.*

70. *DPPA and Privacy*, *supra* n. 65 (". . .in '34 States, someone [could] walk into a State Motor Vehicle Department with your license plate number and a few dollars and walk out with your name and home address.'").

71. 18 U.S.C. § 2721(a) (2000) ("A State department of motor vehicles, and any officer, employee, or contractor thereof, shall not knowingly disclose or otherwise make available to any person or entity: (1) personal information, as defined in 18 U.S.C. 2725(3), about

and "highly restricted personal information."[73] Before the DPPA was enacted, the state DMVs were not only giving out the information to individuals, but many were selling the license holder's personal information to marketing companies, charities, and various political campaigns.[74]

The DPPA however has numerous exceptions, or permissible uses.[75] Many private businesses utilizing swiping believe that their actions are protected by the DPPA exception of a legitimate business use.[76] The private sector may be correct that the DPPA does allow it to use a person's license to verify proof of age where necessary, however, the DPPA does not allow the storage of the individual's personal data in a private database.[77]

---

any individual obtained by the department in connection with a motor vehicle record, except as provided in subsection (b) of this section; or (2) highly restricted personal information, as defined in 18 U.S.C. 2725(4), about any individual obtained by the department in connection with a motor vehicle record, without the express written consent of the person to whom such information applies, except uses permitted in subsections. . . .").

72. 18 U.S.C. § 2725(3) (2000) ("'personal information' means information that identifies an individual, including an individual's photograph, social security number, driver identification number, name, address (but not the 5-digit zip code), telephone number, and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver's status"); Sen. 116, 109th Cong. (Jan. 24, 2005) (stating that the proposed legislation would expand the definition of personal information that could not be released by state DMVs).

73. 18 U.S.C. § 2725(4) ("'highly restricted personal information' means an individual's photograph or image, social security number, medical or disability information"); Sen. 116, *supra* n. 72 (stating that the legislation would expand highly restricted personal information to include an individual's photograph or any physical copy of the driver's license). *Id.* The proposed legislation would also prohibit the disclosure of the personal information of an individual by a private business to a non-affiliated third party unless certain procedures for notice to the individual and an opportunity to restrict the disclosure were followed. *Id.* Finally, the legislation would forbid a private business from requiring an individual from disclosing his or her social security number in order to obtain goods or services. *Id.*

74. Lee, *supra* n. 1 at [¶ 18] ("Before the law was adopted, states were selling driver's license information to direct marketing companies, charities and political campaigns.").

75. 18 U.S.C. § 2721(b) (stating fourteen reasons or exceptions why the information described in 18 U.S.C. § 2721(a) that is not allowed to be disclosed by the DMV may be disclosed). *Id.* The exceptions allowing the use of the information range from the legitimate use of a business in the normal course of business (3), to the use by any private investigator or security personnel (8), to the bulk distribution of surveys or other marketing materials by the State (12).

76. *Id.* at (b)(3)(A). ("For use in the normal course of business by a legitimate business or its agents, employees, or contractors, but only - (A) to verify the accuracy of personal information submitted by the individual to the business or its agents, employees, or contractors").

77. *Research*, *supra* n. 7, at *Is this Legal?* ("Businesses who swipe will most likely say they are protected by this last clause: that swiping is a legitimate business need to verify age and validate a driver's license. But is creating a database from the swiped information for future use and profit a necessity to verify the accuracy of personal information? We'd say no").

C. STATE LAWS

Currently forty-seven states use some type of data encryption method on their driver's license,[78] and thirty-nine of those states use the two dimensional barcode.[79] The DPPA is the only federal regulation on the use of an individual's department of motor vehicles personal information and record.[80] However, a few states have enacted legislation on their own to combat or limit the practice of swiping.[81]

1. *Texas Law*

The Texas statute that went into effect on September 1, 2001,[82] takes a hard-line approach to the issue of private enterprises swiping drivers' licenses to verify age and subsequently retaining the electronically encrypted data. The law, part of the Alcoholic Beverage Code, states that an individual or business may access the electronically encoded information on a driver's license to verify proof of age information in accordance with the code.[83] It further states that the individual or business may not retain the information retrieved from the scan in a database.[84] The information can only be saved if the alcohol commission requires the entity to retain the information.[85] The business may then

78. Positive Access Corporation, *Where it Works*, http://www.positiveaccess.com/where_it_works.html (last updated Aug. 27, 2004) (Currently Alaska, New Jersey, and Wyoming are the only three states that use no type of electronic data encryption process on individual's drivers licenses).

79. *Id.* (In addition to Alaska, New Jersey and Wyoming, which do not use any type of electronic data encryption process on their individual's drivers' licenses; currently California, Florida, Kansas, Michigan, New Mexico, Ohio, Texas, and Vermont use a type of electronic data encryption on their drivers' licenses other than the two-dimensional barcode.).

80. *See Great Taste, Less Privacy*, *supra* n. 1, at [¶ 23] (mentioning only the DPPA when talking about federal protections of drivers' license data), http://www.wired.com/news/print/0,1294,62182,00.html; Lee, *supra* n. 1 at [¶ 17] (mentioning only the DPPA when talking about federal protections of drivers' license data).

81. *Research*, *supra* n. 7, at *Is Swiping Happening in my State?*; Lee, *supra* n. 1 at [¶ 19]; Ill. H. 487, 94th Gen. Assembly (Feb. 10, 2005) (stating that a proposed bill in the most recent Illinois state legislative session would prohibit information from a driver's license from being used for any purpose other than to verify proof of age, including but not limited to selling the information or using the information for any type of solicitations, with the exception that the individual gave express permission so that the information could be used for such purposes).

82. Tex. Alcoholic Bev. Code § 109.61 (2004).

83. *Id.* at § 109.61(a) ("A person may access electronically readable information on a driver's license, commercial driver's license, or identification certificate for the purpose of complying with this code or a rule of the commission, including for the purpose of preventing the person from committing an offense under this code.").

84. *Id.* at § 109.61(b) ("A person may not retain information accessed under this section. . .").

85. *Id.* at § 109.61(b) (". . .unless the commission by rule requires the information to be retained.")

only retain the data for as long as the commission requires.[86] In addition, the retained information may not be marketed in any way.[87] Violation of the statute is a Class A misdemeanor.[88] In Texas, a Class A misdemeanor is punishable by a fine up to four thousand dollars, a jail term of not more than one year, or both the fine and jail term.[89] There has been no challenge to the Texas state law limiting the retention of scanned driver's license data. The Texas Code requires proof of age in order to purchase tobacco products,[90] but it does not address the issue of swiping drivers' licenses to verify the proof of age.

2. *New Hampshire Law*

The New Hampshire law, which was added as an amendment to an existing statute regulating the use of drivers' licenses in 2002,[91] takes an even stricter approach to the issue of scanning and data retention for proof of age purposes. The New Hampshire statute prohibits not only the storing of electronic data encoded on an individual's identification, but it prohibits the swiping of the card to verify age entirely.[92] In addition, the statute acknowledges that swiping may be a better way to verify that the customer's identification is valid and that the holder is of age than merely looking at the card.[93] However, it also states that a seller of alcohol or tobacco who uses due diligence in checking for proof of age, but not swiping the license, will not be held responsible for the acceptance of fraudulent identification.[94] The statute does allow a person to transfer information, in non-electronic form, to another person from the driver's

86. *Id.* at § 109.61(a) ("The person may not retain the information longer than the commission requires").

87. Tex. Alcoholic Bev. Code § 109.61(c) ("Information accessed under this section may not be marketed in any manner").

88. *Id.* at § 109.61(d) ("A person who violates this section commits an offense. An offense under this section is a Class A misdemeanor").

89. Tex. Penal Code § 12.21 (2004) ("An individual adjudged guilty of a Class A misdemeanor shall be punished by: (1) a fine not to exceed $ 4,000; (2) confinement in jail for a term not to exceed one year; or (3) both such fine and confinement").

90. Tex. Health and Safety Code § 161.082(e) (2004).

91. N.H. Rev. Stat. Ann. § 263:12 (2003).

92. *Id.* at § 263:12(X) ("It shall be a misdemeanor for any person to: (X) Knowingly scan, record, retain, or store in any electronic form or format, personal information, as defined in RSA 260:14, obtained from any license, unless authorized by the department").

93. *See generally Id.* at § 263:12(X) (hinting at the fact that the legislature realizes scanning is a more accurate way of checking for valid identification and proof of age, but placing the privacy of its citizens in front of that accuracy).

94. *Id.* at § 263:12(X) ("Notwithstanding any other provision of law, any person selling alcohol or tobacco who uses due diligence in checking identification to prevent unauthorized sales and purchases of alcohol ad tobacco shall not be held responsible for the acceptance of fraudulent identification").

license, but only with the original holder's consent.[95] This means the license holder may give the information to someone else through handwritten or oral means, but not through scanning or swiping.[96] The New Hampshire statute recognizes that there is a better way to verify that drivers' licenses are not fraudulent or expired in determining proof of age, but selects to protect the privacy of its constituent driver's license holders to the utmost degree. The violation of the statute is a class A[97] misdemeanor.[98] In New Hampshire, a class A misdemeanor is punishable by imprisonment, probation, or fine.[99] The legality of this particular section of the statute has not been challenged, and no causes of action have been brought under its authority.

3. *Ohio Law*

Ohio has enacted laws, as of September 21, 2000,[100] that regulate the swiping of identification cards for the purchase of either alcohol or tobacco and for the entry into establishments that serve alcohol.[101] The statutes allow the business employee to perform a "transaction scan"[102]

95. *Id.* at. § 263:12(X) ("Nothing in this paragraph shall prohibit a person from transferring, in non-electronic form or format, personal information contained on the face of a license to another person, provided that the consent of the license holder is obtained if the transfer is not to a law enforcement officer").

96. *See generally* N.H. Rev. Stat. Ann. § 263:12(X) (stating that license data can be collected in non-electronic means).

97. N.H. Rev. Stat. Ann. § 625:9(IV)(a)(2) (2003) ("A class A misdemeanor is. . .(2) Any crime designated within or outside this code as a misdemeanor, without specification of the classification").

98. N.H. Rev. Stat. Ann. § 263:12 ("It shall be a misdemeanor for any person to. . .").

99. N.H. Rev. Stat. Ann. § 651:2(I), (II)(c) (2003) ("(I) A person convicted of a felony or a Class A misdemeanor may be sentenced to imprisonment, probation, conditional or unconditional discharge, or a fine. (II) If a sentence of imprisonment is imposed, the court shall fix the maximum thereof which is not to exceed: (c) One year for a class A misdemeanor.").

100. Ohio Rev. Code Ann. § 2927.021 (Anderson 2004); Ohio Rev. Code Ann. § 4301.61 (Anderson 2004).

101. Ohio Rev. Code Ann. § 2927.021; Ohio Rev. Code Ann. § 4301.61.

102. Ohio Rev. Code Ann. § 2927.021(A)(4) ("'Transaction scan' means the process by which a seller or an agent or employee of a seller checks, by means of a transaction scan device, the validity of a driver's or commercial driver's license or an identification card that is presented as a condition for purchasing or receiving cigarettes or other tobacco products"); Ohio Rev. Code Ann. § 4301.61(A)(4)(a)(b) ("'Transaction scan' means the process by which a permit holder or an agent of employee of a permit holder checks, by means of a transaction scan device, the validity of a driver's or commercial driver's license or an identification card that is presented as a condition for doing either of the following: (a) Purchasing any beer, intoxicating liquor, or low-alcohol beverage; (b) Gaining admission to a premises that has been issued a liquor permit authorizing the sale of beer or intoxicating liquor for consumption on the premises where sold, and where admission is restricted to persons twenty-one years of age or older").

by using a "transaction scan device"[103] to check the validity of the license presented by the customer.[104] If the information deciphered by the scan does not match the information on the license or if the holder is not of proper age, then the employee may not sell that person alcohol, tobacco, or allow admittance into an establishment that serves alcohol.[105] The business may only retain the data of certain specified fields.[106] The business may only store the name,[107] date of birth,[108] and the license expira-

103. Ohio Rev. Code Ann. § 2927.021(A)(5) ("'Transaction scan device' means any commercial device or combination of devices used at a point of sale that is capable of deciphering in an electronically readable format the information encoded on the magnetic strip or bar code of a driver's or commercial driver's license or an identification card"); Ohio Rev. Code Ann. § 4301.61(A)(5) ("'Transaction scan device' means any commercial device or combination of devices used at a point of sale that is capable of deciphering in an electronically readable format the information encoded on the magnetic strip or bar code of a driver's or commercial driver's license or an identification card").

104. Ohio Rev. Code Ann. § 2927.021(B)(1) ("A seller or an agent or employee of a seller may perform a transaction scan by means of a transaction scan device to check the validity of a driver's or commercial driver's license or identification card presented by a card holder as a condition for selling, giving away, or otherwise distributing to the card holder cigarettes or other tobacco products"); Ohio Rev. Code Ann. § 4301.61(B)(1) ("A permit holder or an agent or employee of a permit holder may perform a transaction scan by means of a transaction scan device to check the validity of a driver's or commercial driver's license or identification card presented by a card holder for either of the purposes listed in division (A)(4)(a) or (b) of this section").

105. Ohio Rev. Code Ann. § 2927.021(B)(2) ("If the information deciphered by the transaction scan performed under division (B)(1) of this section fails to match the information printed on the driver's or commercial driver's license or identification card presented by the card holder, or if the transaction scan indicates that the information so printed is false or fraudulent, neither the seller nor any agent or employee of the seller shall sell, give away, or otherwise distribute any cigarettes or other tobacco products to the card holder."); Ohio Rev. Code Ann. § 4301.61(B)(2) ("If the information deciphered by the transaction scan performed under division (B)(1) of this section fails to match the information printed on the driver's or commercial driver's license or identification card presented by the card holder, or if the transaction scan indicates that the information so printed is false or fraudulent, neither the permit holder nor any agent or employee of the permit holder shall sell any beer, intoxicating liquor, or low-alcohol beverage to the card holder").

106. Ohio Rev. Code Ann. § 2927.021(D)(1) ("No seller or agent or employee of a seller shall electronically or mechanically record or maintain any information derived from a transaction scan, except the following . . ."); Ohio Rev. Code Ann. § 4301.61(D)(1) ("No permit holder or agent or employee of a permit holder shall electronically or mechanically record or maintain any information derived from a transaction scan, except the following. . .").

107. Ohio Rev. Code Ann. § 2927.021(D)(1)(a) ("The name. . .of the person listed on the driver's or commercial driver's license or identification card presented by a card holder"); Ohio Rev. Code Ann. § 4301.61(D)(1)(a) ("The name. . .of the person listed on the driver's or commercial driver's license or identification card presented by a card holder").

108. Ohio Rev. Code Ann. § 2927.021(D)(1)(a) ("The. . .date of birth of the person listed on the driver's or commercial driver's license or identification card presented by a card holder."); Ohio Rev. Code Ann. § 4301.61(D)(1)(a) ("The. . .date of birth of the person listed

tion date and identification number of the holder.[109] According to the statute, the information may only be used to prove the performance of a transaction scan, which constitutes an affirmative defense to selling to an underage person.[110] The holder of this information may not share or sell this data to any third party, including any entity for the purposes of marketing, advertising, or promotional activities.[111] The data may only be released to another party pursuant to a court order.[112] If the scanning business stores more data than it is allowed to, or sells that data, it is subject to a civil penalty up to one thousand dollars for each violation.[113] No one has challenged the legality of either statute in a court of law, and no one has brought a case under its authority.

Ohio has also passed legislation that makes the performance of a

---

on the driver's or commercial driver's license or identification card presented by a card holder").

109. Ohio Rev. Code Ann. § 2927.021(D)(1)(b) ("The expiration date and identification number of the driver's or commercial driver's license or identification card presented by a card holder"); Ohio Rev. Code Ann. § 4301.61(D)(1)(b) ("The expiration date and identification number of the driver's or commercial driver's license or identification card presented by a card holder").

110. Ohio Rev. Code Ann. § 2927.021(D)(2) ("No seller or agent or employee of a seller shall use the information that is derived from a transaction scan or that is permitted to be recorded and maintained under division (D)(1) of this section, except for purposes of section 2927.022 [2927.02.2] of the Revised Code"); Ohio Rev. Code Ann. § 4301.61(D)(2) ("No permit holder or agent or employee of a permit holder shall use the information that is derived from a transaction scan or that is permitted to be recorded and maintained by division (D)(1) of this section, except for purposes of section 4301.611 [4301.61.1] of the Revised Code").

111. Ohio Rev. Code Ann. § 2927.021(D)(4) ("No seller or agent or employee of a seller shall sell or otherwise disseminate the information derived from a transaction scan to any third party, including, but not limited to, selling or otherwise disseminating that information for any marketing, advertising, or promotional activities"); Ohio Rev. Code Ann. § 4301.61(D)(4) ("No permit holder or agent or employee of a permit holder shall sell or otherwise disseminate the information derived from a transaction scan to any third party, including, but not limited to, selling or otherwise disseminating that information for any marketing, advertising, or promotional activities").

112. Ohio Rev. Code Ann. § 2927.021(D)(4) (". . .but a seller or agent or employee of a seller may release that information pursuant to a court order or as specifically authorized by section 2927.022 [2927.02.2] or another section of the Revised Code"); Ohio Rev. Code Ann. § 4301.61(D)(4) (". . .but a permit holder or agent or employee of a permit holder may release that information pursuant to a court order or as specifically authorized by section 4301.611 [4301.61.1] or another section of the Revised Code").

113. Ohio Rev. Code Ann. § 2927.021(F) ("Whoever violates division (B)(2) or (D) of this section is guilty of engaging in an illegal tobacco product transaction scan, and the court may impose upon the offender a civil penalty of up to one thousand dollars for each violation"); Ohio Rev. Code Ann. § 4301.61(F) (Whoever violates division (B)(2) or (D) of this section is guilty of an illegal liquor transaction scan, and the court may impose upon the offender a civil penalty of up to one thousand dollars for each violation").

"transaction scan" an affirmative defense to the sale of tobacco[114] or alcohol[115] to an underage person. The business must prove that it took part in several steps in order to claim the affirmative defense.[116] First, the customer must have presented a driver's license or identification card prior to the purchase.[117] Next, the employee must have performed a "transaction scan" on the license that indicated it was valid.[118] Finally, the employee must have reasonably relied on the presentation of the license and the completed "transaction scan" in selling the tobacco[119] or alcohol[120] to the customer. The seller must still exercise reasonable diligence in determining the age of and whether the card presented is that of the customer when examining the license or identification.[121] In Ohio,

114. Ohio Rev. Code Ann. § 2927.022 (Anderson 2004) (stating that the proper performance of a "transaction scan" acts as an affirmative defense to the sale of tobacco to a person not of the legal age to purchase tobacco).

115. Ohio Rev. Code Ann. § 4301.611 (Anderson 2004) (stating that the proper performance of a "transaction scan" acts as an affirmative defense to the sale of alcohol to a person not of the legal age to purchase alcohol).

116. Ohio Rev. Code Ann. § 2927.022(A) ("A seller or an agent or employee of a seller may not be found guilty of a charge of a violation of section 2927.02 of the Revised Code in which the age of the purchaser or other recipient of cigarettes or other tobacco products is an element of the alleged violation, if the seller, agent, or employee raises and proves as an affirmative defense that all of the following occurred"); Ohio Rev. Code Ann. § 4301.611(A) ("A permit holder or an agent or employee of a permit holder may not be found guilty of a charge of a violation of this chapter or any rule of the liquor control commission in which the age of a purchaser of any beer, intoxicating liquor, or low-alcohol beverage is an element of the alleged violation, if the permit holder, agent, or employee raises and proves as an affirmative defense that all of the following occurred").

117. Ohio Rev. Code Ann. § 2927.022(A)(1) ("A card holder attempting to purchase or receive cigarettes or other tobacco products presented a driver's or commercial driver's license or an identification card"); Ohio Rev. Code Ann. § 4301.611(A)(1) ("The card holder attempting to purchase any beer, intoxicating liquor, or low-alcohol beverage presented a driver's or commercial driver's license or an identification card").

118. Ohio Rev. Code Ann. § 2927.022(A)(2) ("A transaction scan of the driver's or commercial driver's license or identification card that the card holder presented indicated that the license or card was valid"); Ohio Rev. Code Ann. § 4301.611("A transaction scan of the driver's or commercial driver's license or identification card that the card holder presented indicated that the license or card was valid").

119. Ohio Rev. Code Ann. § 2927.022(A)(3) ("The cigarettes or other tobacco products were sold, given away, or otherwise distributed to the card holder in reasonable reliance upon the identification presented and the completed transaction scan").

120. Ohio Rev. Code Ann. § 4301.611 ("The beer, intoxicating liquor, or low-alcohol beverage was sold to the card holder in reasonable reliance upon the identification presented and the completed transaction scan").

121. Ohio Rev. Code Ann. § 2927.022(B)(1)-(2) (". . .[T]he use of a transaction scan device does not excuse a seller or an agent or employee of a seller from exercising reasonable diligence to determine, the following: (1) Whether a person to whom the seller or agent or employee of a seller sells, gives away, or otherwise distributes cigarettes or other tobacco products is eighteen years of age or older; (2) Whether the description and picture appearing on the driver's or commercial driver's license or identification card presented by a card

the business owner cannot be held liable for selling tobacco or alcohol to an underage person if all of these criteria are met.

4. *Connecticut Law*

Connecticut has laws, enacted in 2003, regulating scanning that are very similar to the regulations in Ohio. In Connecticut, a "transaction scan device"[122] may be used to perform a "transaction scan"[123] in order to determine the customer's age before the purchase of alcohol[124] or tobacco.[125] The business may only record the patron's name, date of birth, and the expiration date from the license or identity card.[126] These data fields may then be stored in a database for use as an affirmative defense

---

holder is that of the card holder"); Ohio Rev. Code Ann. § 4301.611(B)(1)-(2) (". . .[T]he use of a transaction scan device does not excuse a permit holder or an agent or employee of a permit holder from exercising reasonable diligence to determine, the following: (1) Whether a person to whom the permit holder or agent or employee of a permit holder sells any beer or intoxicating liquor is twenty-one years of age or older or sells any low-alcohol beverage is eighteen years of age or older; (2) Whether the description and picture appearing on the driver's or commercial driver's license or identification card presented by a card holder is that of the card holder").

122. Conn. Gen. Stat. § 30-86(a)(4) (2003) ("'Transaction scan device' means any commercial device or combination of devices used at a point of sale that is capable of deciphering in an electronically readable format the information encoded on the magnetic strip or bar code of a driver's license or an identity card"); Conn. Gen. Stat. § 53-344(4) (2003) ("'Transaction scan device' means any commercial device or combination of devices used at a point of sale that is capable of deciphering in an electronically readable format the information encoded on the magnetic strip or bar code of a driver's license or an identity card.").

123. Conn. Gen. Stat. § 30-86(a)(3) ("'Transaction scan' means the process by which a permittee or permittee's agent or employee checks, by means of a transaction scan device, the validity of a driver's license or an identity card"); Conn. Gen. Stat. § 53-344(3) ("'Transaction scan' means the process by which a seller or seller's agent or employee checks, by means of a transaction scan device, the validity of a driver's license or an identity card.").

124. Conn. Gen. Stat. § 30-86(c)(1) ("A permittee or permittee's agent or employee may perform a transaction scan to check the validity of a driver's license or identity card presented by a cardholder as a condition for selling, giving away or otherwise distributing alcoholic liquor to the cardholder").

125. Conn. Gen. Stat. § 53-344(d)(1) ("A seller or seller's agent or employee may perform a transaction scan to check the validity of a driver's license or identity card presented by a cardholder as a condition for selling, giving away or otherwise distributing tobacco to the cardholder").

126. Conn. Gen. Stat. § 30-86(d)(1) ("No permittee or permittee's agent or employee shall electronically or mechanically record or maintain any information derived from a transaction scan, except the following: (A) The name and date of birth of the person listed on the driver's license or identity card presented by a cardholder; (B) the expiration date and identification number of the driver's license or identity card presented by a cardholder"); Conn. Gen. Stat. § 53-344(e)(1) (2003) (No seller or seller's agent or employee shall electronically or mechanically record or maintain any information derived from a transaction scan, except the following: (A) The name and date of birth of the person listed on the driver's license or identity card presented by a cardholder; (B) the expiration date and identification number of the driver's license or identity card presented by a cardholder").

in the instance of a sale to a minor, as long as the employee reasonably relied on the scan.[127] The business may not disseminate the stored information to any third parties for marketing, advertising, or promotional activities.[128] The information may only be released pursuant to a court order.[129] A civil penalty not to exceed one thousand dollars shall be imposed per instance for anyone who releases the information without such a court order.[130] Again, neither of these statutes has been challenged in a court of law, and no one has brought a lawsuit under the statutes.

5. *Other State Laws*

Several other states have proposed, enacted and repealed, or enacted minimal regulating legislation dealing with scanning. Paralleling both Ohio and Connecticut laws, New York actually passed legislation, effective in 1999, which expressly granted a business the right to perform a "transaction scan"[131] on a customer's license before selling them

127. Conn. Gen. Stat. § 30-86(d)(1) ("In any prosecution of a permittee or permittee's agent or employee for selling alcoholic liquor to a minor in violation of subsection (b) of this section, it shall be an affirmative defense that all of the following occurred: (A) A cardholder attempting to purchase or receive alcoholic liquor presented a driver's license or an identity card; (B) a transaction scan of the driver's license or identity card that the cardholder presented indicated that the license or card was valid; and (C) the alcoholic liquor was sold, given away or otherwise distributed to the cardholder in reasonable reliance upon the identification presented and the completed transaction scan"); Conn. Gen. Stat. § 53-344(f)(1) ("In any prosecution of a seller or seller's agent or employee for a violation of subsection (b) of this section, it shall be an affirmative defense that all of the following occurred: (A) A cardholder attempting to purchase or receive tobacco presented a driver's license or an identity card; (B) a transaction scan of the driver's license or identity card that the cardholder presented indicated that the license or card was valid; and (C) the tobacco was sold, given away or otherwise distributed to the cardholder in reasonable reliance upon the identification presented and the completed transaction scan").

128. Conn. Gen. Stat. § 30-86(d)(3) ("No permittee or permittee's agent or employee shall sell or otherwise disseminate the information derived from a transaction scan to any third party for any purpose, including, but not limited to, any marketing, advertising or promotional activities"); Conn. Gen. Stat. § 53-344(e)(3) ("No seller or seller's agent or employee shall sell or otherwise disseminate the information derived from a transaction scan to any third party, including, but not limited to, selling or otherwise disseminating that information for any marketing, advertising or promotional activities").

129. Conn. Gen. Stat. § 30-86(d)(3) (". . .a permittee or permittee's agent or employee may release that information pursuant to a court order."); Conn. Gen. Stat. § 53-344(e)(3) (". . .a seller or seller's agent or employee may release that information pursuant to a court order").

130. Conn. Gen. Stat. § 30-86(d)(5) ("Any person who violates this subsection shall be subject to a civil penalty of not more than one thousand dollars."); Conn. Gen. Stat. § 53-344(e)(5) ("Any person who violates this subsection shall be subject to a civil penalty of not more than one thousand dollars").

131. N.Y. Alcoholic Bev. Control Law § 65-b(1)(c) (2004) ("'Transaction scan' means the process involving a device capable of deciphering any electronically readable format by which a licensee, or agent or employee of a licensee under this chapter reviews a driver's

alcoholic beverages.[132] The scanning of the identification card before the purchase worked as an affirmative defense[133] for the employee, provided that "reasonable diligence" was exercised in the transaction.[134] For the affirmative defense claim, the business could only store the necessary identity fields of name, date of birth, driver's license or identification card number, and expiration date.[135] The entity could not sell or provide the data to any third party for advertising, marketing, or promotional purposes.[136] The information could only be released pursuant to a court order or some other type of statutory need.[137] Violation of the statute was a civil penalty punishable by a fine not to exceed one thousand dollars.[138] The statute is however no longer in effect today.[139] The legislature enacted the statute as an amendment to an existing alcoholic beverage control law, and included an expiration of January 1, 2004 devoid of renewal.[140] The legislature failed to renew the scanning sections, and did not enact any subsequent legislation to replace it. Therefore,

---

license or non-driver identification card presented as a precondition for the purchase of an alcoholic beverage as required by subdivision two of this section or as a precondition for admission to an establishment licensed for the on-premises sale of alcoholic beverages where admission is restricted to persons twenty-one years or older").

132. *Id.* at § 65-b(2)(b) ("Upon the presentation of such driver's license or non-driver identification card issued by a governmental entity, such licensee or agent or employee thereof may perform a transaction scan as a precondition to the sale of any alcoholic beverage").

133. *Id.* at § 65-b(7)(a) ("In any proceeding pursuant to subdivision one of section sixty-five of this article, it shall be an affirmative defense that such person had produced a driver's license or non-driver identification card apparently issued by a governmental entity, successfully completed the transaction scan, and that the alcoholic beverage had been sold, delivered or given to such person in reasonable reliance upon such identification and transaction scan").

134. *Id.* at § 65-b(7)(a) ("Use of a transaction scan shall not excuse any licensee under this chapter, or agent or employee of such licensee, from the exercise of reasonable diligence otherwise required by this section").

135. *Id.* at § 65-b(7)(b) ("A licensee or agent or employee of a licensee may electronically or mechanically record and maintain only the information from a transaction scan necessary to effectuate the purposes of this section. Such information shall be limited to the following: (i) name, (ii) date of birth, (iii) driver's license or non-driver identification number, and (iv) expiration date").

136. N.Y. Alcoholic Bev. Control Law § 65-b(8) ("No licensee or agent or employee of a licensee shall resell or disseminate the information recorded during such scan to any third person. Such prohibited resale or dissemination includes, but is not limited to, any advertising, marketing or promotional activities").

137. *Id.* at § 65-b(8) ("Notwithstanding the restrictions imposed by this subdivision, such records may be released pursuant to a court ordered subpoena or pursuant to any other statute that specifically authorizes the release of such information.").

138. *Id.* at § 65-b(8) ("Each violation of this subdivision shall be punishable by a civil penalty of not more than one thousand dollars").

139. *Id.* at § 65-b.

140. *Id.* at § 65-b.

currently in New York, the practice of scanning licenses and storing the information is once again unregulated.

California's legislature proposed and discussed scanning laws in 2003.[141] The California Assembly discussed and amended a bill that would have put restrictions on who could scan, and on what information could be stored and for how long.[142] However, the bill never passed as a limitation on scanning. Oddly enough, the California legislature amended the bill and passed it as a roof coverings law.[143] California then also remains unregulated with respect to scanning.

A few other states have enacted legislation that does not regulate scanning, but does incorporate it either as an affirmative defense to criminal or civil suit or as a punishment. West Virginia has enacted legislation that allows a business that has installed a transaction scan device on its premises to use the performance of a transaction scan as an affirmative defense to the sale of alcohol or tobacco to a minor.[144] The state obviously allows scanning tacit in the statute's existence alone, but there is nothing in any law regulating data retention or use.[145] Finally, Oregon has developed the most unique use for scanning. The state allows scanning without any regulation on data recording or use.[146] What is different is that Oregon has a statute that instead of imposing a fine or suspension of liquor license for selling alcohol to a minor, allows the state to force the business to "acquire and use equipment designed to prevent sales of alcoholic beverages to minors."[147] Oregon actually uses scanning technology as a means to punish businesses that have sold alcohol to underage persons in the past.

D. Fair Information Practice Principles

Since the U.S. became a sovereign nation, the need to protect the privacy of Americans has been a concern of the government.[148] With the development of new technology the need for protection does not decrease,

141. *Electronic Reading*, *supra* n. 10.

142. *Id.*

143. 2004 Cal. Stat. 318.

144. W. Va. Code § 60-3A-25a (2004).

145. *Id.* at § 60-3A-25a.

146. Or. Rev. Stat. § 471.342 (2003).

147. *Id.* at § 471.342.

148. *See* U.S. Const. amend. I (recognizing a right to privacy as to which religion a person selects, what a person says in his or her speech, and in what the press publishes); U.S. Const. amend. IV (recognizing a right of privacy amongst the people so that the government cannot enter their houses to search them or seize items without the proper authority); *Roe v. Wade*, 410 U.S. 113, 152 (realizing that the Constitution does not explicitly mention a right to privacy, but that through certain amendments and subsequent case law on those amendments a right of privacy has been recognized).

it only changes form.[149] With every new technological invention, such as scanning, new privacy issues arise that must be addressed.[150]

For more than thirty years, the government has been analyzing privacy concerns in the technology age.[151] In 1973, as the computer began to be realized and widely used, the United States Department of Health, Education, and Welfare's Advisory Committee on Automated Personal Data Systems developed the first "fair information practices."[152] The report acknowledged that with the advent of computers people's information could be stored in a way that it could not be in the past.[153] The records would be much easier to store in a computer system and access than in the past with only paper.[154] This was the first realization that computers were changing the collection of information, and in turn, privacy concerns would change as well.[155]

In more recent years, with the development of the Internet and more information being gathered online, the privacy principles have been up-

149. *See FTC Report*, *supra* n. 6 (describing that with the advent of electronic record keeping the ability to collect and access personal data became much easier, and therefore new standards needed set forth to regulate this new process).

150. *See generally* Lee, *supra* n. 1 (addressing numerous security and privacy issues that have arisen from scanning).

151. *See* U.S. Dept. of Health, Educ., and Welfare, Recs, *Computers and the Rights of Citizens*, 73-94 (July, 1973) (This report discusses privacy of personal information with the advent of electronic data collection and storage devices, and it is more than thirty years old).

152. *Id.* at sec. IV(III) (Among other regulations offered for the protection of information the report detailed six rights of individual data subjects that are similar to the current "Fair Information Practice Principles." The regulation calls for any organization that maintains an automated data system to (1) inform the individual asked to supply personal data whether he or she is legally required to do so, and to provide known consequences for providing or not providing the data, (2) inform the individual, upon request, whether he or she is the subject of data within the system, and provide the data to the individual if he or she so desires it, (3) assure that the data in the system is not used in a manner other than that stated to the individual without his or her consent, (4) inform the individual, upon his request, about the uses of his or her data, and identify all people or organizations involved with the system, (5) assure no data on the individual is made available by means of a compulsory legal process, unless the individual has been notified of the demand, and (6) maintain procedures that (i) allow the individual to contest the information's accuracy, pertinence, completeness, and necessity to retain, (ii) amend or correct data when the individual so requests, (iii) assure that when there is a dispute with an individual over a correction or amendment to the data that the individual's claim is recorded and included in any subsequent disclosures or disseminations of information); Jonathon P. Cody, Student Author, *Protecting Privacy Over the Internet: Has the Time Come to Abandon Self-Regulation?*, 48 Cath. U. L. Rev. 1183, 1204 (1999).

153. *See generally* Recs, *Computers and the Rights of Citizens*, *supra* n. 151 (acknowledging that new technology allowed information to be stored and accessed in much more efficient ways than in the past).

154. *Id.*

155. *Id.*

dated. In June of 1998, the United States Federal Trade Commission ("FTC") presented a report to Congress detailing what has become known as the "Fair Information Practice Principles" for the online gathering of data.[156] The FTC determined that there are five core principles that all online information gatherers should follow to assure the person whose information is being collected is sufficiently informed of the practice.[157] The principles include: (1) notice/awareness, (2) choice/consent, (3) access/participation, (4) integrity/security, and (5) enforcement.[158] The report addressed these five principles and concluded that most websites were collecting online data from consumers, but were not providing notice of the practice to them.[159] Although in violation of the principles, the report acknowledged that without enforcement, the Web sites would go unregulated and the practice would continue.[160]

III. ANALYSIS

The information encrypted on drivers licenses has many uses that are both useful and worrisome. Law enforcement officers perform one commendable use of swiping.[161] Police officers can use the card scanning technology to both save time and money in writing citation reports and retrieving suspect background information.[162] Private enterprises also use the technology of swiping in beneficial ways for both society and for the benefit of the individual business. By scanning the ID, the business can immediately tell if the card is valid and if the holder is over the age needed to purchase either alcohol or cigarettes.[163] This is beneficial to society because it cuts down on the amount of underage people who purchase alcohol, cigarettes, or gain entry into bars by illegally using fake identification.[164] The bars and convenience stores then often store

156. Cody, *supra* n. 152 at 1209-1210; Jordan M. Blanke, *"Safe Harbor" and the European Unioin's Directive on Data Protection*, 11 Albany L.J. of Sci. & Tech. 57, 69-70 (2000).

157. Cody, *supra* n. 152, at 1209-1210; Blanke, *supra* n. 156, at 70-72.

158. Cody, *supra* n. 152, at 1210; Blanke, *supra* n. 156, at 70-72; *FTC Report*, *supra* n. 6, at III(A).

159. Blanke, *supra* n. 156, at 69-70.

160. *FTC Report*, *supra* n. 6, at III(A)(5)(a)-(c) (stating that the three types of regulation for online gathering of data that allow the user redress are (a) "self-regulation" by the industry itself, (b) "private remedies" including legislation, and (c) "government enforcement" that would be either civil or criminal in nature).

161. *Great Taste, Less Privacy*, *supra* n. 1, at [¶ 12], http://www.wired.com/news/print/0,1294,62182,00.html.

162. *Id.* at [¶ 12], http://www.wired.com/news/print/0,1294,62182,00.html (stating police officers scan the driver's license during a traffic stop in order to produce an electronic citation report and to retrieve the suspect's background information).

163. Christiansen, *supra* n. 2 at [¶ 6]; *Research*, *supra* n. 7, at *Who is Swiping?*.

164. *See* Christiansen, *supra* n. 2 (describing the way swiping technology is cutting down on the amount of underage people purchasing alcohol and cigarettes, and stating implicitly how this is beneficial to society).

the data in a computer database that can be very beneficial to the business for marketing purposes.[165] The business can then use the marketing record to determine what type of patrons come on certain nights, to direct market to certain customers, and even to reject the admittance of certain troublesome individuals.[166]

Along with all the beneficial uses of the electronic information, there are certain problem areas where security and privacy issues arise. Problem areas arise when the private enterprises begin collecting the data for marketing purposes.[167] Most drivers' licenses have at least as much data electronically encrypted as printed on them, and many have much more.[168] This information is much different in the possession of private individuals from the control of law enforcement officers.[169] Law enforcement officers are generally considered some of society's most upstanding citizens who would not misuse the private information he or she is privileged to obtain. They undergo rigorous background checks and deal with sensitive data constantly to prepare them to handle exposure to such confidential information.[170] However, private citizens are a different story.

When individuals are allowed to easily access and store very private and personal information, many dangers arise.[171] The first is the danger of an employee using the data as an aid to commit violent crimes such as stalking, rape, or even murder.[172] In addition, identity theft is becoming more of a problem in our society everyday, and with this much personal

---

165. Lee, *supra* n. 1 at [¶¶ 21-27].

166. *Id.* at [¶¶ 14-16, 31].

167. *See generally Great Taste, Less Privacy*, *supra* n. 1, http://www.wired.com/news/print/0,1294,62182,00.html (describing how personal data is collected through transaction scans and problems that arise when that data is subsequently used for marketing purposes).

168. *Id.* at [¶ 11], http://www.wired.com/news/print/0,1294,62182,00.html (stating some states have social security numbers embedded on licenses, and Kentucky has encrypted a digital image of the holder's picture on the license); *Research*, *supra* n. 7, at *What Information is Encoded on Drivers' Licenses?* (stating some states have digital fingerprints, signatures, and photos electronically embedded on licenses).

169. *See generally Great Taste, Less Privacy*, *supra* n. 1, http://www.wired.com/news/print/0,1294,62182,00.html (citing the police uses for information obtained through swiping and commending them, while at the same time criticizing private enterprise uses of the information gained through transaction scans).

170. *See Of Taxes and Duties*, *infra* n. 198, at 366 n. 74.

171. *Great Taste, Less Privacy*, *supra* n. 1, at [¶¶ 23-24], http://www.wired.com/news/print/0,1294,62182,00.html.

172. *See Id.* at [¶ 23], http://www.wired.com/news/print/0,1294,62182,00.html (stating that employees may access the personal data and compile lists of customers that could be used to commit violent crimes).

information available the temptation and risk abounds.[173] Finally, but not as serious a threat, is the thoughts of receiving even more annoying marketing phone calls, mail, or other direct marketing material.[174] There are also few security measures built into the process to protect customers' information.

Currently some of the scanning manufacturers and some of the states who produce the drivers' licenses include security features to stop identity theft or violent crime. A few of the manufacturers of the scanning equipment include security features that are supposed to protect the consumers' private information.[175] These measures are questionable though. Some of the data on electronically encoded licenses is also encrypted in such a way that only law enforcement officers can access it, but with higher security levels coming into effect after 9/11 that could soon be changing to allow private industries access.[176]

There are also questions raised as to what people's rights to privacy are under the Fair Information Practice Principles.[177] In order for a business to collect and use personal information, it should follow these guidelines to assure the individual's privacy is protected.[178] These guidelines include; (1) giving notice to the individual that the information is being collected, (2) getting the person's consent or giving him/her a choice as to how the information may be used, (3) allowing the person to access the data about himself/herself to assure that it is accurate and complete, (4) to assure that the data is safeguarded and secure, and finally (5) that there is some type of recourse to enforce the guidelines.[179]

All of the beneficial uses of the information by private entities raise concerning questions involving the privacy and safety of the general public that must be analyzed. Some type of legislation should be enacted, not to completely prohibit the use of scanning by private businesses, but to affirmatively limit the amount of personal information that can be accessed and retained by these entities. Scanning or swiping is a new means of private entities getting your personal information. If the prac-

173. *See Id.* at [¶ 24], http://www.wired.com/news/print/0,1294,62182,00.html (stating that the Center for Democracy & Technology said that the potential for identity theft and fraud are high at businesses that scan).

174. *Swiping driver's licenses*, *supra* n. 1, at [¶¶ 1-3], http://www.seattlepress.com/print-10148.html.

175. *Frequently Asked Questions*, *supra* n. 52.

176. *Id.* (acknowledging that although the data is almost always encrypted in a way to limit access to law enforcement agencies and other official uses that in a post 9/11/2001 world "certain private security uses of such data may be permitted by new laws and regulations as we go forward").

177. *FTC Report*, *supra* n. 6, at III.

178. *Id.*

179. *Id.*

tice is not addressed and regulated privacy in this area may be a thing of the past.

A. Beneficial Uses of Scanning

1. *Law Enforcement Uses*

Law Enforcement officials perform one very beneficial use of swiping drivers' licenses to access electronically encoded data.[180] Law enforcement officers can use the technology in conjunction with private businesses to locate or obtain information about suspects.[181] Officers are also able to take advantage of the technology in the field to improve their own safety, expedite a routine traffic stop and subsequent citation, and by doing so make society safer.[182]

Private enterprise scanning really assists law enforcement in two ways. First, when a business swipes a license, the time and date of the transaction scan are recorded along with the personal information.[183] This data can then be used to aid law enforcement officers in apprehending suspects. If a law enforcement officer calls or visits a business with demographic information of a suspect, the business could instantly run a database query to determine if the person had been to the business recently.[184] Also, a police department could call the business with only a name or social security number to see if the name is in the private

180. *Great Taste, Less Privacy*, *supra* n. 1, at [¶ 10], http://www.wired.com/news/print/0,1294,62182,00.html (stating that scanning licenses makes life easier for law enforcement officers and makes them more efficient); Bob Howie, *Oak Ridge to update court software; Old system slows processing of information*, The Houston Chronicle Sec. This Week Pg. 3 (June 24, 2004) (discussing that scanning enables a police officer to save time and write citations more efficiently); *Electronic Citation Systems*, *supra* n. 16, at *Introduction* (acknowledging that law enforcement officer who swipe are more efficient, and provide better safety for society while also increasing their own safety).

181. Lee, *supra* n. 1 at [¶ 10] (stating that law enforcement officers can call private businesses to see if certain names or social security numbers appear on their customer lists); *see generally Great Taste, Less Privacy*, *supra* n. 1, at [¶ 15], http://www.wired.com/news/print/0,1294,62182,00.html.

182. *Electronic Citation Systems*, *supra* n. 16; *Oak Ridge to update court software; Old system slows processing of information*, *supra* n. 180, at [¶¶ 6-9] (illustrating how a police officer can use the technology to decrease the time taken for a routine traffic stop); *Great Taste, Less Privacy*, *supra* n. 1, at [¶ 12], http://www.wired.com/news/print/0,1294,62182,00.html (stating that scanning makes life easier for law enforcement officers).

183. *Great Taste, Less Privacy*, *supra* n. 1, at [¶ 15], http://www.wired.com/news/print/0,1294,62182,00.html (illustrating how when a person comes into a business and their license is swiped that the scanning equipment records the time and date of the transaction in addition to the encoded license data).

184. Lee, *supra* n. 1 at [¶ 10] (illustrating that the equipment has already proved useful in law enforcement because police departments have called bars with names and social security numbers to see if the information shows up on the customer list.).

database, and then access this information.[185] Law enforcement could use a private database to access a person's address, telephone number, or other personal information. Both of these uses allow law enforcement to work more efficiently in apprehending suspects and makes society a safer place, but is not without drawbacks. Under these circumstances and uses, some argue that a de facto national identity card and national personal information database would then be created.[186] If the police did not have your information, they could just call local bars, restaurants, and convenience stores until they found it. The most alarming thought is that the database would not be controlled by the government, but by corporate America.

A second, and less controversial use, by law enforcement officers of swiping takes place by police officers in the field. Many officers are equipped with either handheld PDA-style computers or laptops that are connected to informational databases through wireless Internet connections.[187] The computer has software on it that allows the officer to merely swipe the offender's driver's license and instantly have the citation report information filled in.[188] The citation is then printed by a handheld printer the officer also carries.[189] The officer saves a great deal of time and reduces the chance for human error by not having to manually write in the criteria required on the citation.[190] He or she is able to get back onto the streets to patrol much faster.[191] The patrolman also improves his or her own safety by not having to take his or her eyes off of the offender for several minutes to manually write out a citation, the scanning only takes a few seconds.[192]

The mobile computers can also access informational databases over wireless Internet connections.[193] This allows the officer to scan the offender's license to instantly check his or her background information.[194] The officer can discover if the person has a history of offenses, or if he or

185. *See generally Id.* at [¶ 10] (If a law enforcement officer can use a bar's database to discover if a suspect has recently visited the establishment, then the law enforcement officer could just as easily, and as a logical next step in apprehension, use the bar to obtain all of the customer's data from the database retained.).

186. *Id.* at [¶ 11] (discussing that privacy advocates argue that a de facto national security card or internal passport is being created that will be registered in numerous databases); *Great Taste, Less Privacy*, *supra* n. 1, at [¶ 26], http://www.wired.com/news/print/0,1294,62182,00.html.

187. *Electronic Citation Systems*, *supra* n. 16, at 1-2.

188. *Id.* at 1-2.

189. *Id.* at 1-2.

190. *Id.* at 6-7.

191. *Id.* at 6-7.

192. *Electronic Citation Systems*, *supra* n. 16, at 6-7.

193. *Id.* at 1-2.

194. *Id.* at 6-7.

she has any outstanding warrants.[195] All of this is done in real time for the freshest most up to date information available, allowing the officer to be as safe and efficient as possible.[196] The scanning also allows the officer to instantly access very basic information such as if the license is valid, if the offender is a minor, etc.[197] This could help in identifying some adult offenders, and would be especially helpful in identifying minors guilty of committing certain age related offenses such as underage drinking, smoking, or curfew violations.

Overall, the use of scanning by law enforcement officers should be encouraged, and is one of the intended uses for electronically encoded information on drivers' licenses. The practice makes society safer, and more efficient. There is very little risk that a police officer is going to keep the offender's data to commit a violent crime against him, or to steal his identity. Law enforcement officers often deal with sensitive personal data, but they have underwent a thorough background check and are sworn to an oath to uphold the law to assure they are people who can be trusted with such information.[198] Employees and owners of private businesses are not subject to the same type of precautionary measures, and are not viewed in the same way. Therefore, sensitive personal information in the hands of a law enforcement officer is much different than in the possession of a private business.

2. *Private Business*

Many private businesses that must check the age of their patrons or customers for the purchase of alcohol or tobacco are currently using scanning technology.[199] The technology not only helps decrease human error and customer wait time, but it exponentially increases the chances that an underage person will be identified and prevented from purchasing al-

---

195. *Id.* at 6-7.

196. *Id.* at 6-7.

197. *See generally Electronic Citation Systems*, *supra* n. 16, at 1-2 (If all of the person's background information can be checked when the license is scanned, then the scanner could also determine if the license is fraudulent, and if the holder is a minor).

198. *See* Kenneth H. Ryesky, *Of Taxes and Duties: Taxing the System with Public Employees' Tax Obligations*, 31 Akron L. Rev. 349, 366 n. 74 (1998) (citing the fact that a police officer undergoes a rigorous background check and is sworn to uphold the law. . . "Those in law enforcement have a heightened duty to obey all the laws and to set an example for others, not to brazenly declare that they are somehow above the law. . .").

199. Chung, *supra* n. 1 at 443; Lee, *supra* n. 1 at [¶¶1-4]; *Great Taste, Less Privacy*, *supra* n. 1, at [¶ 13], http://www.wired.com/news/print/0,1294,62182,00.html (realizing that bars and restaurants scan IDs to catch underage drinkers, and convenience stores scan them verify the age of cigarette buyers); Christiansen, *supra* n. 2, at [¶¶ 5-6].

cohol or tobacco.[200] Many bars, restaurants, liquor stores, and convenience stores now employ the technology to help stop the purchase and consumption of alcohol and tobacco by underage persons.[201] The businesses can also store the electronic information in computerized customer databases.[202] The information can then be used for marketing purposes, to analyze the client base, or to aid law enforcement officers by keeping a record of when people visited certain locations.[203]

Underage drinking is a large problem in many areas, but with the use of barcodes and magnetic strips with electronically encoded data on them and with more scanning devices being used by bars, the problem is diminishing.[204] Many underage people are able to purchase high-quality, fraudulent identification cards that allow them to purchase alcohol and gain admittance to bars.[205] The new technology allows the business owners to either swipe the magnetic strip or scan the barcode in order to instantly access the encoded data and determine if the license is valid and the age of the holder.[206] With the scanning equipment, the business is able to determine an identification card is fake that would probably otherwise pass a physical examination by an employee.[207] It is virtually impossible to produce a license with a fraudulent magnetic strip or barcode.[208] Many convenience store owners are using the technology to attack the similar problem of underage people attempting to purchase

200. Chung, *supra* n. 1 at 443 (acknowledging that scanning helps reduce human error, reduces the wait time of patrons wanting to purchase alcohol or tobacco or gain entry into a bar, and automatically detects underage persons or fraudulent identification).

201. *Id.* at 443 (citing the fact that numerous private entities are scanning, and more begin the practice each day).

202. *Id.* at 443 (stating that the bar's management may retain the scanned customer information in its own customer database).

203. Lee, *supra* n. 1.

204. *See* Christiansen, *supra* n. 2 (The same underage woman gained access to a saloon on numerous occasions using a fake ID. After the saloon employed the use of swiping technology, the ID was confiscated and she was denied access.).

205. *Id.* at [¶ 3] (illustrating that underage college students can often purchase high-quality fraudulent IDs for less than $100); Roger Johnson, *F.A.B. IDs: Detecting Fake, Altered, and Borrowed Cards*, Law Enforcement Bulletin, Focus on Training, [¶ 5] (February 1997) (available online at http://www.fbi.gov/publications/leb/1997/feb972.htm) (A study on the prevalence of underage people who have fraudulent identification discovered that as many as twenty-two percent of University of Wisconsin at Madison students have false identification cards allowing them to purchase alcohol and enter bars. Some University of Wisconsin police officers estimate the number of students possessing fake identification cards to be as high as fifty percent).

206. Christiansen, *supra* n. 2, at [¶¶ 6-7] (illustrating that the machines can automatically tell if the ID is real because if it is not an error message will appear on the screen).

207. *Id.* at [¶ 21] (stating that many fake IDs sold are of "good quality" and could pass all the validity checks except the ones using the bar codes and magnetic strips).

208. *See generally Id.* (stating that the only way that many fake IDs are detected is by scanning them).

alcohol or tobacco.[209]

Another benefit, particularly for bar and restaurant owners, is the storing of the electronic data in computer databases for marketing purposes.[210] An owner can instantly create charts that show statistics of patrons who visit on certain nights.[211] For example a bar owner can run a query to see what the male to female ratio is on a given night, or to see what age most of the people are who come in to watch a certain musical performance.[212] This information can then be used to market future similar performances to those patrons or similar patrons, or to attempt to change customer balances on certain nights by running different promotions.[213] The data is also very lucrative in negotiating with alcohol companies over promotions.[214] Convenience stores can use similar technology to build databases for direct marketing purposes.[215]

The practice of directly marketing customers has advantages for society. Patrons are able to receive notice of events that match their specific interests.[216] In the past where people may have missed certain events because they did not know of them, now there would be a direct means of contact to alert a customer of musical performances, promotional events, or other activities that the person would find interest-

209. Chung, *supra* n. 1 at 443 (citing that an increasing amount of convenience stores are relying on scanning technology to avoid illegal sales of alcohol or tobacco to minors).

210. Lee, *supra* n. 1, at [¶¶ 21-27].

211. *Id.* at [¶¶ 21-27].

212. *Id.* at [¶¶ 21-27] (giving examples of how bar owners use the scanning technology to pinpoint the demographics of their crowds on certain nights). *Id.* A bar owner uses the database to determine that on Tuesdays, the amount of forty-something patrons increases because of the jazz music being played. *Id.* On Thursdays, the crowd is almost entirely from the upscale Boston ZIP codes of 02109, 02111, and 02113 who come to hear the band Cat Tunes, a band well known among those who visit Martha's Vineyard. *Id.* On Sundays women make up sixty percent of the customers because Chad LaMarch performs, and "[t]he men always follow the women." *Id.*

213. *Id.* at [¶¶ 21-27] (stating the information can be used to look at crowd demographics or to give customers who frequent the establishment special treatment, similar to the way an airline would give extra benefits to a frequent flier).

214. *Id.* at [¶¶ 21-27] (discussing how the demographic information can be valuable to the owner of the club). *Id.* The statistics can be used to show an alcohol supplier the demographics of the customer base for a certain night in order to gain leverage for the bar owner in terms of promotions. This information can be used to guarantee the supplier has the people it wants at a certain promotion, and it will in turn be worth more money to the supplier to pay the bar owner to run the promotion on a certain night.

215. Lee, *supra* n. 1, at [¶¶ 21-27] (quoting an owner of over 100 convenience stores in Minnesota and Wisconsin who recently installed scanning technology in all of his convenience stores: "Any marketing tool that we have that makes us different than our competition is an advantage . . . [w]e could do direct marketing to people who are smokers. . . .").

216. *Id.* at [¶¶ 21-27]; *Swiping driver's licenses*, *supra* n. 1 at [¶ 3], http://www.seattlepress.com/print-10148.html.

ing.[217] The situation would resemble having a socialite friend who knew your specific tastes in addition to the local entertainment scene and could alert you of events you would want to attend.

Allowing the private entities to collect only non-identifiable data for marketing or customer demographic purposes is another option. Business owners would be able to collect demographic data such as age, weight, sex, zip code, city, etc.; but nothing identifiable such as name, address, social security number, driver's license identification number, etc. This would still enable businesses to determine what type of customer and from where the customer was patronizing,[218] but would not allow any type of personal identifiable data to be transmitted. For example a bar owner could see what the ratio of male-to-female customers was on Friday night, or see what age most of the people were that visited on Tuesday night from the information.[219] However, there would be no personal identifiable information to allow direct marketing to these recent customers, so the information would be of limited use. The customers would be protected from the dangers of identity theft and violent crime associated with divulging personal information though, because there would be no information in the database to personally identify them.

Finally, there are some security controls that are beneficial to the storeowner, and also to law enforcement.[220] A bar owner that wants to keep a troublesome patron from entering the establishment can simply program the computer to reject his or her license.[221] Since the time and date are recorded when the license is swiped, the business owners can also use this information to assist law enforcement officers.[222] All of these uses benefit many people; however, the benefits of these scenarios do not outweigh the dangerous side effects of allowing private enterprises to collect sensitive data that is not necessary to accomplish their primary purpose of age verification.

---

217. *See generally* Lee, *supra* n. 1, at [¶¶ 21-27] (describing how a bar owner can discern the demographics on any particular night in order to advertise certain events to individuals who are in certain demographic groups); *Swiping driver's licenses*, *supra* n. 1 at [¶ 4], http://www.seattlepress.com/print-10148.html (describing how a club could use personal information collected from a transaction scan to pinpoint that person's interests and in turn market certain bands or other types of performances directly to that person).

218. Lee, *supra* n. 1, at [¶¶ 21-27]; *Swiping driver's licenses*, *supra* n. 1 at [¶ 4].

219. *See generally* Lee, *supra* n. 1, at [¶¶21-27] (stating how a club owner can use the collected data to survey what demographic groups visit the establishment on certain nights or for certain events).

220. *Id.* at [¶¶ 10, 31].

221. *Id.* at [¶ 31] (giving the example that simply "knowing that a quarrelsome man is named Greg and lives in a specific town can be enough information to lock someone out").

222. *Id.* at [¶ 10] (stating explicitly that law enforcement officers could call a bar to see if a suspect's name or social security number show up on the customer list, and implicitly that the law enforcement officer could then obtain whatever data the business held on that particular person).

B. Side-Effects of Scanning

1. *Violent Crime*

Although there are many beneficial uses to swiping and to businesses creating customer databases, there are also many dangers of having extremely private information in the hands of private individuals.[223] The most dangerous of all the risks is the possibility the database information could be used for the commission of violent crimes.[224] All the societal benefits gained through businesses restricting underage patrons and marketing via swiping and data retention could be offset by the commission of one rape or murder.[225]

The amount of personal information businesses that swipe IDs store in their private databases is startling.[226] Some of the businesses store addresses, phone numbers, social security numbers, and any other information that can be decoded by the scanner from the license.[227] The security of the databases themselves and the software used to run them is also questionable.[228] Most bar employees can access the data, and subsequently use it for their own purposes.[229]

A few scanning manufacturers are aware of the problems of personal information being abused and only allow clients to view and store certain encoded data.[230] The problem here, though, is that the equipment man-

---

223. *Great Taste, Less Privacy*, *supra* n. 1, http://www.wired.com/news/print/0,1294,62182,00.html.

224. *See generally Id.* at [¶ 23] (implying that after a bar or restaurant employee made a list of female patrons' personal information that list could be used not just for stalking, but for other criminal purposes).

225. *See generally Id.* (stating that there is a possibility of an employee of a business that scans creating a personal list of customer information from the entity's customer database, and that the DPPA was enacted because people used the state DMVs to obtain personal information to commit murder or other crimes).

226. *See generally Id.* at [¶¶ 1-5] (citing an experiment where patrons at an event had their licenses swiped and afterward were alarmed by the amount of information that was obtained from this swipe).

227. Chung, *supra* n. 1 at 443 (illustrating that licenses contain data including name, address, birth date, height, eye color, and social security number, and that many private businesses retain this data from a transaction scan); Lee, *supra* n. 1, at [¶¶ 2-4] (stating that name, address, birth date, height, eye color, and social security number can be electronically encoded on licenses and that this personal information can be stored in a computer database following a transaction scan).

228. *See generally* Lee, *supra* n. 1, at [¶¶ 23-38] (citing no security precautions taken by private business owners who scan and subsequently store personal data).

229. *See generally Id.* at [¶¶ 23-38] (citing no security measures that bar or restaurant owners take to ensure that only employees who should have access to the personal data are the only ones who have access to the data).

230. *Id.* at [¶ 36] (giving examples of how some scanning technology manufacturers limit the amount of information their clients have access to in order to protect the patron's safety). *Id.* (The Logix Company (a scanner manufacturer) only allows clients like bars to

ufacturer has no more need or right to the data than does their client. It becomes a situation akin to inmates running the prison.

A majority of companies, however, allow businesses to store all of the database information locally, with all employees gaining easy access.[231] With the information stored locally, there is little to stop an employee from creating personal lists of potential victims to stalk, rape, or murder.[232] An employee of a bar, for example, could create a list of blond female customers between the ages of twenty-one and twenty-five that weigh 120 pounds that includes all of their contact information.[233] The thought of someone doing this purely for stalking purposes is scary enough, but far worse crimes could occur.[234] The DPPA was in fact passed for the very reason of an obsessed fan receiving address information on Rebecca Schaeffer from the DMV that he used to stalk and murder her.[235] Some businesses may not even look at the stored information, or may use it in a proper manner.[236] However, some will not use the data responsibly, so action to prevent such abuses must be taken.[237] The only way to stop the people who will use the information incorrectly is to regulate what information can be accessed and stored by everyone. The alternative could result in severe consequences for innocent customers of not just violent crime, but also of having their entire bank account emptied or credit ruined through identity theft.

2. *Identity Theft*

Another threat to patrons when their personal information is obtained by private entities is identity theft. It is an ever-increasing phe-

---

view aggregate information and not specific data to prevent a situation where "a bouncer at a bar stalks a blond, 20-year-old, 5-foot-7 girl." A sales manager with Logix Company stated, "[a]s a company we want to take responsibility for who has responsibility for this information").

231. *Id.* at [¶ 37] (stating that Intelli-Check, and most manufacturers, allow their clients to store all customer data locally).

232. *Great Taste, Less Privacy*, *supra* n. 1, at [¶ 23], http://www.wired.com/news/print/0,1294,62182,00.html.

233. *Id.* at [¶ 23] (giving another example of how a bar employee could create a list of all the blond female customers who are between the ages of 21 and 25 who weigh 120 pounds for stalking or other violent crime purposes).

234. *See generally Id.* at [¶ 23] (stating implicitly that since a crazed fan obtained information about Ms. Schaeffer that was used to murder her from the state DMV that an employee of a private business who scans and retains a customer database could just as easily obtain such data from the entity's database).

235. *Id.*

236. Lee, *supra* n. 1, at [¶¶ 37-39] (quoting a bar owner who uses the scanning technology: "Will I use it in the wrong way? No. But then again, what is to stop the next guy?").

237. *Id.* at [¶¶ 37-39].

nomenon in the United States,[238] which demonstrates no signs of stopping or slowing down.[239] Currently more than seven million people are the victim of identity theft in the United States every year.[240] That equals the startling number of more than thirteen thefts per minute.[241] The total cost of this crime in the United States approaches fifty billion dollars.[242] Allowing private enterprises to continue to scan drivers' licenses and retain the data could increase the identity theft statistics. These businesses scan drivers' licenses that contain very personal data; the type of data that people attempting to commit identity theft wish to acquire.[243]

The driver's license is often the means through which an identity thief can best procure the identity.[244] In addressing the issue of identity theft, the California legislature stated that "identity theft is often 'facilitated through the procurement of a counterfeit or fraudulently-obtained driver's license since the license is a 'breeder document' for all sorts of assets and benefits: loans, bank accounts, credit cards, etc.'[245] '[T]he driver's license remains an attractive tool for identity thieves and will no doubt continue to be the target of those seeking to commit fraud.'"[246] By allowing private enterprises to retain all the information encrypted on a driver's license, the opportunity for someone to use this data for identity theft is far too easy.

The potential for fraud in the storing of the information is great because of the ease that third parties can acquire the data.[247] Since a two-dimensional barcode and magnetic strip can be read with a handheld

238. *Id*entity Theft Resource Center, *Facts & Statistics*, http://www.idtheftcenter.org/facts.shtml at [¶ 3] (last updated Feb. 15, 2004) (showing the amount of identity theft victims increased between eleven and twenty percent from the year 2001 to the year 2002, and the amount of victims increased eighty percent from the year 2002 to the year 2003).

239. *Id.* at [¶ 3] (stating that ninety-one percent of people do not see an end to identity theft, and actually expect a heavy increase in the number of victims).

240. *Id.* at [¶ 3] (last updated February 15, 2004) (according to two studies performed in July 2003, seven million people had their identity stolen in the United States since July 2002).

241. *Id.* at [¶ 3] (last updated February 15, 2004) (showing that if seven million people had their identity stolen in the United States between July 2002 and July 2003 that equaled 19,178 thefts per day, 799 per hour, and 13.3 per minute).

242. Federal Trade Commission, *Identity Theft Survey Report*, http://www.ftc.gov/os/2003/09/synovatereport.pdf, at 6 (September, 2003).

243. *See generally* Cal. Assembly Comm. on Jud. 224, p. 4, 2003-2004, (Mar. 4, 2003) (stating that the information contained on drivers' licenses is the type of data that an identity thief would want to acquire, and that a drivers' license is a "breeder document" for access to numerous assets and benefits).

244. *Electronic Reading*, *supra* n. 10 at 4; *Swiping driver's licenses*, *supra* n. 1 at [¶ 4].

245. *Electronic Reading*, *supra* n. 6, at 4.

246. *Id.* at 4.

247. *Id.* at 4; *Great Taste, Less Privacy*, *supra* n. 1, at [¶ 24], http://www.wired.com/news/print/0,1294,62182,00.html (stating that the potential for fraud and identity theft is

scanner, an employee can scan the license a second time with a personal scanner to generate a copy of the information.[248] He could then use the stored data either to commit an identity theft, or sell the data to someone else who would like to commit such a crime.[249] Obtaining the equipment needed for scanning is very simple, and there are no perquisites required for purchase.[250] Most scanning manufacturers have websites where the equipment can be purchased for as little as few hundred dollars.[251] All that is required is a valid credit card, a mailing address, and name for online purchases.[252] Not very many identities must be stolen, or information for the theft need to be sold to recoup this minimal expenditure.[253]

Employees may obtain the data for identity theft purposes in other manners. Even if the card is swiped via fixed position swiping technology, the information is still accessible.[254] Some equipment produces a written receipt of the transaction, and almost all systems present a digital display of the encoded information.[255] An employee or someone standing nearby could take the receipt, copy the receipt, or write down

high for businesses that perform transaction scans according to the Center for Democracy & Technology).

248. *Great Taste, Less Privacy*, *supra* n. 1, at [¶ 24], http://www.wired.com/news/print/0,1294,62182,00.html (stating that since many private entities use handheld scanners it would be easy for an employee to purchase a handheld scanner of his or her own and scan a license twice, the second time retaining the data for his or her own benefit).

249. *See generally Id.* (stating implicitly that once the employee scans a license a second time for his own benefit that the employee would then use the information to commit identity theft or sell the information to someone who would commit such a theft).

250. Token Works, *Store*, http://www.cardvisor.com/default.htm (last accessed Nov. 12, 2004).

251. *Id.* (showing that the scanners can be purchased for relatively small sums of money). *Id.* Handheld scanners, which come with software to store swiped data, are priced as little as three hundred and ninety-five dollars. This model (CardVisor I) will only read magnetic stripes and only stores license number, date of birth, expiration date, status of the swipe, and date and time of the swipe. The model measures only 1" x 6" x 3" and runs for 6,000 plus scans on two standard AAA batteries. Models that are more expensive capture and store the aforementioned fields as well as contact information such as name, title, address, city, state, zip, and gender. Models that also read two-dimensional barcodes are available starting at $1,145 dollars (CardVisor II-BC).

252. *Id.* at *Store* (illustrating the simplicity and low cost of obtaining a handheld scanner to perform transaction scans on licenses by an ordinary person).

253. *See generally Identity Theft Survey Report*, *supra* n. 242, at 6 (stating that the average identity thief fraudulently obtains $10,200 worth of goods and services in the commission of each theft). *Id.* If the average identity thief obtains $10,200 worth of goods and services from every commission of a theft, and the cost of scanning equipment is only a few hundred dollars, then it takes less than one "average" theft to not only recoup the cost of the scanning equipment, but also to make a hefty profit.

254. *Electronic Reading*, *supra* n. 10 at 4.

255. *Id.* at 4.

the information for later personal or sales use.[256] Finally, if the information is stored in a database, an employee could access the data and use it for identity theft, or sell it to a third party who would like to commit identity theft.[257] Individuals' scanned data is usually transferred onto an ordinary desktop or laptop computer, the access to which only the business controls.[258]

The more information a person has the easier it is to commit identity theft.[259] For example if an identity thief has a driver's license number, name, address, age, height, weight, etc., all information usually electronically encoded on a license, the thief can "steal" an identity in a couple different ways. First, he could use the obtained information in an attempt to gain access to existing credit cards, bank accounts, or other personal financial funds.[260] Second, the thief could also use the information to create an entirely new and fraudulent driver's license that could be used to open any number of credit cards or bank accounts.[261] Since some states encode data that is even more personal, such as social security number, on their licenses for the establishments to collect, it makes the thief's job that much easier. The risks to a person's life, financial security, and credit history are far too great to have such extremely private information in the possession of people who do not absolutely require it.

3. *Direct Marketing*

Another telemarketing phone call, mailbox full of "junk-mail", or an e-mail account full of "spam" e-mail is life in the twenty-first century. A third, but less serious result of scanning and storing the data from a

256. *See generally Id.* at 4 (stating that the identifying information of a customer could easily be obtained by a third party even if the business entity scanning does not share it via the scanning equipments printout or display).

257. *See generally Id.* at 4 (stating that the driver's license is an attractive document for identity thieves because the information contained on it is very valuable in gaining access to private assets or benefits); *Great Taste, Less Privacy*, *supra* n. 1, at [¶ 24], http://www.wired.com/news/print/0,1294,62182,00.html (commenting on how easy it would be for an employee of an establishment that swiped to take the personal information and sell it to a third party).

258. *See* Token Works, *FAQ*, http://www.cardvisor.com/default.htm (last accessed Nov. 12, 2004) (stating that although a computer is not required, the device will download the data to an ordinary desktop or laptop in Microsoft Excel format).

259. *See generally Electronic Reading*, *supra* n. 10 at 4 (hinting at the fact that the more information that is contained on a driver's license, the more information an identity thief can procure from such license, and the easier it is for the thief to then steal the identity).

260. *See Id.* (listing items that an identity thief may be able to access with the information from a driver's license, including loans, bank accounts, and credit cards); *Plouff asks, "What's in a name?,"* *supra* n. 259 at [¶ 6] (acknowledging the fact that with the driver's license information criminals can access a person's credit, or worse yet start new credit in that person's name).

261. *Id.*

customer's driver's license is the increase of direct marketing that a person will receive.[262] Although some of the marketing material may be useful to the patron such as coupons, discounts, or information about special performances,[263] a majority will result in more headaches for an already overloaded audience when it comes to direct marketing. A majority of the material the customer receives will end up in the trash, blocked by a "spam" blocker, or as a deleted message on an answering machine. The nuisance of more marketing is not appealing; especially at the risk of privacy invasion, violent crimes, or identity theft. The sum total of all three risks necessitates that regulations be imposed, particularly because present technical safeguards are insufficient to protect the public.

C. EQUIPMENT SAFEGUARDS

Some of the equipment used in scanning, and some of the licenses themselves are supposed to have security features built into them that would prevent the private information encoded on drivers' licenses from falling into the wrong person's hands.[264] Certain highly sensitive material, such as biometric information, is supposedly encrypted in a way that most ordinary scanners cannot read it.[265] Other states, such as Illinois, claim they encode the license data in a way that only the Secretary of State's office or a law enforcement officer can read the biometric data.[266] With the advent of newer scanning technology and new laws in our society's ever increasing struggle for security this information may become accessible to private businesses.[267] In a recent exhibition using scanning equipment available to the general public information includ-

262. *Great Taste, Less Privacy*, *supra* n. 1, at [¶¶ 14-16], http://www.wired.com/news/print/0,1294,62182,00.html; Lee, *supra* n. 1 at [¶¶ 21-31]; *Swiping driver's licenses*, *supra* n. 1 at [¶ 4]; Chung, *supra* n. 1 at 443.

263. *Swiping driver's licenses*, *supra* n. 1 at [¶ 4]; Lee, *supra* n. 1 at [¶¶ 21-31]; Chung, *supra* n. 1 at 443.

264. *Frequently Asked Questions*, *supra* n. 52, at q. 8; Lee, *supra* n. 1 at [¶¶ 32-37].

265. *Frequently Asked Questions*, *supra* n. 52, at q. 8 (describing that driver's license biometric data is almost always encrypted to allow only law enforcement officers and official users access); Lee, *supra* n. 1 at [¶¶ 32-33] (stating that most scanning equipment is not designed to read biometric information such as digital fingerprints, digital signature, and electronic photographs).

266. CyberDrive Illinois, *New Look. . . New Technology! Illinois' New Driver's Licenses and ID Cards*, http://www.sos.state.il.us/departments/drivers/programs/digital.html (last accessed October 30, 2004) (alerting people that the encrypted data of the new Illinois driver's license and identification card can only be accessed by the Secretary of State's office and by law enforcement).

267. *Frequently Asked Questions*, *supra* n. 52, at q. 8 (acknowledging that in the wake of 9/11/2001 "new laws and regulations may allow the private uses of biometric data to help increase security"); *Great Taste, Less Privacy*, *supra* n. 1, at [¶¶ 1-9], http://www.wired.com/news/print/0,1294,62182,00.html.

ing phone number, income range, marital status, housing value, address, and profession were obtained from scanning drivers' licenses.[268] Scanning technology and the laws are advancing too rapidly to leave the sensitive biometric data unregulated, or poorly regulated as is currently the case by the individual states, in its capture.

Some scanning equipment manufacturers recognize there is a privacy and safety issue with personal information being made available to private businesses.[269] The Logix Company, for example, is a manufacturer of swiping technology that self-regulates the information that some of its clients have access to.[270] The company does not allow clients like bars to view specific data, but only aggregate customer information.[271] The data is stored offsite in a Logix database so it can regulate what the bars can access.[272] The self-regulation is commendable in the acceptance of the scanning equipment provider that there is a privacy issue, and trying to prevent it. However, it does not get around the problem that the Logix company still has a database of the entire bar customers' private information. The scanning equipment manufacturer has no more right to access the data than the bar owner. Most equipment dealers do not implement this practice anyway, and the business owner is allowed to store and access any data so chosen.[273]

---

268. *Great Taste, Less Privacy*, *supra* n. 1, at [¶¶ 1-9], http://www.wired.com/news/print/0,1294,62182,00.html (giving an example of how easily personal information can be obtained from the license itself or from the information contained on the license). *Id.* An exhibition at the Pittsburgh Center for the Arts was held by a private enterprise, which used scanners that are available to the general public to scan driver's licenses. The enterprise was able to decode information off the license that amounted to or led to the discovery of phone numbers, income range, marital status, housing value, profession, and address. The license contained enough data that the enterprise could use a commercial data mining service or voter registration to gain access to the remainder of the information not included on the card.

269. Lee, *supra* n. 1 at [¶¶ 36-39]; *See Electronic Reading*, *supra* n. 10 at 4 (realizing that some scanning systems only allow the user to calculate the cardholder's age and the equipment only displays a "yes purchase" or "no purchase" indication, but other systems allow the user to print out information and store information in a database).

270. Lee, *supra* n. 1 at [¶ 36]; Memphis Business Journal, *Concord EFS acquires Logix*, http://www.bizjournals.com/memphis/stories/2002/03/04/daily1.html, [¶ 10] (Mar. 4, 2002.).

271. *Id.* at [¶ 36] (accepting that a situation where a bouncer at a bar could get information on a twenty year old five-foot-seven blond girl and then stalk her, the Logix company only allows clients like bars to view aggregate customer data and not user specific personal information).

272. *Id.* at [¶ 36-37] (inferring that because of the way Logix Company only allows certain data to be accessed by bars, it must not allow client data storage on site). *Id.* The Logix Company only allows certain information to be accessed by its clients. The author then states that most manufacturers allow the information to be stored locally. Therefore, the Logix Company must not allow data storage on site.

273. *Id.* at [¶ 36-37] (Most companies, like Intelli-Check, allow the clients to store all the license data locally, which allows them easy access to specific data).

The only way equipment safeguards could really regulate scanning was if there was an industry standard or regulation that limited the amount of information that could be obtained and stored off identification cards; or if all the states encoded private data in a way that scanners could not read it. It is unlikely manufacturers will change their equipment to only decode certain data voluntarily though, because many equipment manufacturers actually advertise their products as being able to store mass quantities of customer information for marketing purposes.[274] There would also still be a problem because there would be countless older technology scanners that could decode private data still in the possession of business owners. It would be very difficult, if not impossible, for the industry itself to regulate the use of this previously sold equipment.

The states regulating themselves, as far as encoding private data so a scanner cannot decode it, is another option. All fifty states producing licenses that encode personal data so it cannot be read by scanners is more probable, but still difficult. It would be difficult to have uniform standards. One state may believe that an information field is private and encode it, but other states may not. Since scanning equipment cannot think, the state a license is from does not matter, the scanner will detect all fields it is capable of detecting. Some states also may decide not to encode any of their data. These difficulties would leave some state's citizens protected, and others not. Federal regulations would be much more uniform, and efficient. A Federal regulation would force all states to follow it. The self-regulation of encoding drivers' licenses so scanners cannot read certain data, or leaving the burden on scanning manufacturers to regulate themselves is not the best way to make scanning a beneficial yet safe practice.

D. Fair Information Practice Principles

Although the core fair information practice principles were developed for the online collection of data, the similarities between collecting and using data from online consumers and scanning licenses to obtain data are enough to implement the principles to the practice. The Internet allows for the low cost, efficient, and vast collection of information from individuals.[275] The same is true with the advent of scanning of drivers licenses. In the past if someone wanted to collect data off a drivers license, he would either have to write it down or make a photocopy of it. Some argue that swiping is no different than making a copy of some-

274. Token Works, *Products*, http://www.cardvisor.com/default.htm (last accessed Nov. 12, 2004).

275. *FTC Report*, *supra* n. 6, at VI.

one's license,[276] but it is far different. Copying a license is a process that a person would be aware of, and the data would still be just on a piece of paper unless it was entered into a database. Scanning, on the other hand, makes the collection of the data much easier, it is already in electronic format, and very often people are misled about what the data will be used for or that it will be used at all.[277] The same is true of Internet data collection. People often enter private information about themselves for online uses without knowing for exactly what purposes the information will be used.[278] The only difference is that with online information gathering, the individual at least knows what information he or she is releasing that could possibly be misused. With scanning, people often do not even know their license contains encoded information, let alone that the business who just asked for their license is taking it for their own use. The process of scanning in most places is currently in violation of the fair information practice principles. Without some type of a mechanism to enforce the core principles though, they are ineffective.

1. *Notice/Awareness*

The first core principle of fair information practice is notice or awareness.[279] Consumers should be given notice that information is being collected from them, otherwise they cannot make an informed decision as to what information they would like to disclose, if any.[280] As well, if there is no notice given to the consumer then three of the other principles, choice/consent, access/participation, and enforcement/redress are not meaningful.[281] The scope and content of notice depends on the substantive information practices of the entity collecting data, but the following have been recognized as essential to assuring consumers are aware they are divulging information:

- identification of the entity collecting the data;
- identification of the uses to which the data will be put;
- identification of any potential recipients of the data;

276. *Great Taste, Less Privacy*, *supra* n. 1, at [¶ 17], http://www.wired.com/news/print/0,1294,62182,00.html.

277. *Id.* at [¶ 17-18].

278. *FTC Report*, *supra* n. 6, at VI (giving examples of how online merchants obtain data without notifying the person supplying the information exactly how the data will be used). *Id.* For example, an automobile dealership advertises on its website that it can help consumers fix their credit rating. To take advantage of the offer consumers are asked to provide their name, address, social security number, and telephone number on an online information form. The website says nothing about how the information will actually be used, or if the information will become available to third parties.

279. *Id.* at III(A)(1).

280. *Id.* at III(A)(1).

281. *Id.* at III(A)(1).

- the nature of the data collected and the means by which it is collected if not obvious;
- whether the provision of the requested data is voluntary or required, and the consequences of a refusal to provide the requested information; and
- the steps taken by the data collector to ensure the confidentiality, integrity and quality of the data.[282]

Currently, most business entities who swipe or scan licenses are not giving their customers any indication that the devices are actually storing data and not just checking the patron's age.[283] The consumer is not told who will have access to the data, how it will be used, or the security features involved to protect the data.[284] Customers also have little control over what information they disclose in a transaction scan. Some places do not allow people admittance or sales if they choose not to have their card swiped,[285] while others will.[286] However, a business cannot pick and choose what information fields to scan and retain for each individual customer. Submitting to a transaction scan will surrender all data that device is programmed to record.[287] For these reasons, businesses are not satisfying the notice element of the core principles by alerting customers of the transaction scan process.

2. *Choice / Consent*

The second core principal is choice or consent as to how the collected data is used.[288] The customer must have some type of choice as to how

282. *Id.* at III(A)(1).

283. *Great Taste, Less Privacy*, *supra* n. 1, at [¶ 18], http://www.wired.com/news/print/0,1294,62182,00.html ("The policy is that you shouldn't be collecting the info for one purpose and using it for another. If you're telling them you're using it to verify their age, you shouldn't be using it to market them"); Lee, *supra* n. 1 at [¶¶ 2-3] (admitting that most customers are not aware that scanning pulls up not just proof of age, but also name, address, birth date, and other personal information); Hong Chung, *supra* n. 1 at 443 (acknowledging that most patrons do not realize the amount of information stored on their license that businesses may be collecting and storing in a database for marketing use).

284. *Great Taste, Less Privacy*, *supra* n. 1, at [¶ 18], http://www.wired.com/news/print/0,1294,62182,00.html; Lee, *supra* n. 1 at [¶¶ 2-3]; Chung, *supra* n. 1 at 443.

285. *Swiping driver's licenses*, *supra* n. 1 at [¶ 4] (citing that many private entities make it very difficult for a customer to prohibit their license from being swiped and still gain admittance or sales, and that many businesses condition sales on the ability of the entity to swipe the card).

286. *Great Taste, Less Privacy*, *supra* n. 1, at [¶ 19-22], http://www.wired.com/news/print/0,1294,62182,00.html (Andy Rose, the manager of the West End restaurant in Little, Rock Arkansas, scans and retains data from licenses. He has witnessed some customers "raise hell" over having their license swiped. He subsequently states that if a patron objects, the bar does not insist on scanning the identification, and still allows admittance).

287. *See generally Products*, *supra* n. 274 (describing the information that the card readers can detect).

288. *FTC Report*, *supra* n. 6, at III(A)(2).

the information collected is used after the transaction is completed.[289] When an entity scans a license choice is not an issue because there is no notice to the customer that the information is being collected.[290] Without notice, there can be no choice.[291] There must be both notice and consent for a consumer to be adequately protected under the Fair Information Practice Principles.

3. *Access / Participation*

The third practice principle is access to the data stored or participation in its storage.[292] Individuals must have the ability to access the personal records stored and to contest the information's accuracy and completeness.[293] Once again, because here the customer does not have notice that the information is being collected, access or participation is inappropriately nullified.[294]

4. *Integrity / Security*

The fourth core principle is the integrity or security that the information stored is accurate and secure. Customers' data must be protected by the source collecting it.[295] There must be no unauthorized disclosure or use for unauthorized purposes of the data.[296] The business must take reasonable steps such as providing the customer access to the data, and destroying untimely data. Although the entities collecting the data collect and utilize the records in different ways, it can be safely assumed that not all establishments are taking the necessary steps to secure the data. Since most scanners store the data in a basic format, such as Microsoft Excel, that can be downloaded onto a computer,[297] the real gatekeeper of the records becomes the business owner. Since there are numerous types of entities using transaction scans to check identification and store the data, it is unknown what types of precautions these business owners are taking. Possibilities include only the owner having access to the computer that stores the data, limiting access to just the management, or allowing all employees access. However businesses are or are not limiting who has access to the data, it is very likely that not all entities are adequately protecting the information.

289. *Id.* at III(A)(2).
290. *Id.* at III(A)(1).
291. *Id.* at III(A)(1).
292. *Id.* at III(A)(3).
293. *FTC Report*, *supra* n. 6, at III(A)(3).
294. *Id.* at III(A)(1).
295. *Id.* at III(A)(4).
296. *Id.* at III(A)(4).
297. *FAQ*, *supra* n. 258.

5. *Enforcement/Redress*

The fifth, and final, principle is enforcement or redress by the customer.[298] The FTC stated that "[i]t is generally agreed that the core principles of privacy protection can only be effective if there is a mechanism in place to enforce them."[299] Absent some type of enforcement, the fair information practice principles are no more than a suggestive guideline.[300] Currently there is no redress for someone whose information is obtained and used unfavorably as a result of scanning.

E. The Future

Swiping of drivers' licenses to gain entry into bars and restaurants, as well as to purchase alcohol or tobacco, is already an established practice and becomes more widespread everyday.[301] However, here it appears that "technology has outpaced the law, and the casualty is privacy."[302] Although some states have enacted legislation to prevent or restrict the use of scanning and data retention, an overwhelming majority of states have no regulation of swiping whatsoever. On a national level, the federal government has not even addressed the issue. This is an issue that has too great of a public policy concern for the federal government to sit idly by while citizens privacy rights continue to be violated. One of the reasons the national government is in place is to protect and provide for the general welfare of the citizens.[303] Allowing private businesses to force consumers to trade their private personal information, which can be used to commit crimes or identity theft against them, is not protecting citizens. There should be federal legislation enacted to regulate swiping.

There is a great deal of information already encoded on most state's licenses, and with the advent of better technology, there will be even more in the future. Digital fingerprints, digital signatures, and digital photographs are just a few of the fields some state licenses now include. This is information that a private business neither needs access to in order to verify age, nor for any other reason would it be entitled to this information. The only information a private entity needs to check proof of age is the holder's date of birth, license expiration, license number, and name. With this information the employee checking the card can

298. *Id.* at III(A)(5).

299. *Id.* at III(A)(5).

300. *Id.* at III(A)(5).

301. Chung, *supra* n. 1 at 443 (stating that in the United States an ever increasing amount of businesses are using scanning technology to verify age of customers attempting to purchase alcohol and tobacco).

302. *Swiping driver's licenses*, *supra* n. 1 at [¶ 1].

303. U.S. Const. art. 1, § 8, cl. 1 ("The Congress shall have the Power To. . .provide for the Common Defence and general Welfare of the United States. . .").

verify the license is valid, that the holder is over the age required, and can compare the person to the picture on the license to verify he or she is the holder of the license presenting it. The holder's address, social security number, height, weight, or other information is not needed to verify age, and would not make the age validation process any more accurate. The amount of information should be limited to protect consumer privacy. The few marketing benefits to the business of obtaining this information are highly outweighed by the serious risks of violent crime and identity theft that the consumer is exposed to by surrendering such data. The scanning equipment manufacturers should not be relied upon to restrict the amount of information to which their clients have access to, because they should not have access to increased information either. The same possibilities for harm and privacy concerns exist if the manufacturers have access to the information as if the businesses do.

A business should be allowed to store the name, date of birth, license expiration and license number information in a database if it so desires, but only for the assertion of an affirmative defense to the charge to transacting business with a minor. This limited storage would be similar to the Ohio[304] and Connecticut[305] statutes that allow the storage of a limited amount of data only for the assertion of an affirmative defense.[306] Also in accordance with both of these states' statutes, the business would not be allowed to disseminate or sell the information to any third parties, or to use the information for direct marketing purposes.[307] Finally, if the private entity wishes to perform transaction scans and/or store the data, then the business must comply with the fair information practice principles in doing such. In other words, customers must be given: (1) notice that the practice is taking place, (2) consent to the transaction, (3) access to the stored data if requested to assure its accuracy, (4) security of the data collected, and (5) enforcement if the process is not followed or the data is misused. Even this limited amount of information is sensitive and must be protected to the utmost degree.

To protect the welfare of the public the penalties for breaking the new law should be flexible, but strict. Fines, suspension or revocation of the business license, and possible prison sentence is a good mixture of regulation. Depending on the type of information collected, the way it was used, and the length of time or amount of information collected the punishment would vary. For instance, if addresses were being collected for internal marketing use this may only be a fine the first time, and a

304. Ohio Rev. Code Ann. § 2927.021; Ohio Rev. Code Ann. § 4301.61.

305. Conn. Gen. Stat. § 30-86; Conn. Gen. Stat. § 53-344.

306. Conn. Gen. Stat. § 30-86(e); Conn. Gen. Stat. § 53-344(f); Ohio Rev. Code Ann. § 2927.022; Ohio Rev. Code Ann. § 4301.611.

307. Conn. Gen. Stat. § 30-86(d)(3); Conn. Gen. Stat. § 53-344(e)(3); Ohio Rev. Code Ann. § 2927.021(D)(4); Ohio Rev. Code Ann. § 4301.61(D)(4).

possible suspension of business license the second time. If information that is more private were collected, like social security numbers or digital signatures, then a first offense may result in a suspension of business license, and a second infraction may end in incarceration.

Congress has the authority to enact such legislation from a Constitutional standpoint. The Commerce Clause[308] allows Congress to regulate interstate commerce, and in conjunction with the Necessary and Proper Clause[309] Congress may enact legislation that it deems necessary and proper to carry out what is defined in the Commerce Clause.[310] Since alcohol and tobacco are both items that move in interstate commerce and the actual purchasers of such goods may be from other states, then Congress would be allowed to enact legislation regulating its sale.[311] Congress also has the power to enact legislation affecting the use of personal information included on drivers' licenses because it enacted the DPPA.[312] Therefore, it would have the power to enact legislation regulating scanning of licenses or identification cards to verify proof of age. This activity should not be left to the states in this situation because it is evident the states are not acting quickly enough to address the issue, and because the lack of uniformity in the few existing state statutes would make any hope of future uniformity in state enacted scanning regulations doubtful. Future federal legislation may look similar to this:

> 101-1. Sales of alcohol and tobacco to minors. Use of transaction scan device as affirmative defense.
>
> (a) Definitions:
>
> (1) "Card holder" means any person who presents a driver's license, commercial driver's license, or identification card in order to purchase or receive alcohol products or tobacco products from a seller or agent or employee of the seller; or any person who presents a driver's license, commercial driver's license, or identification card to a permittee or agent of employee of the permittee in order to gain admittance to a social establishment that sells, gives away, or otherwise distributes alco-

308. U.S. Const. art. 1, § 8, cl. 3 ("Power of Congress to regulate commerce. To regulate commerce with foreign nations, and among the several states, and with the Indian tribes.").

309. U.S. Const. art. 1, § 8, cl. 18 ("All necessary and proper laws. To make all Laws which shall be necessary and proper for carrying into Execution the foregoing Powers, and all other Powers vested by this Constitution in the Government of the United States, or in any Department or Officer thereof").

310. *McCulloch v. Maryland*, 17 U.S. 316 (1819) (describing how Congress has the power to enact legislation not expressly set forth in the Constitution by combining the Necessary and Proper Clause with another enumerated power, such as the Commerce Clause).

311. *Katzenbach v. McClung*, 379 U.S. 294 (1964) (finding that even though most of the customers of Ollie's Barbecue were not traveling in interstate commerce, the business was still involved in interstate commerce because a portion of its food had traveled in interstate commerce, and some of its patrons had also traveled in interstate commerce).

312. 18 U.S.C. § 2721.

holic beverages or tobacco products.[313]
(2) "Identification card" means a state or federal issued identification card that has electronically encoded data stored on it.[314]
(3) "Social establishment" means a business, club, or other entity that under other regulations is required by law to check for proof of age before selling, giving away, or otherwise distributing alcohol or tobacco products to its customers. Social establishments include, but are not limited to, bars, clubs, taverns, certain restaurants, cigar bars, etc.[315]
(4) "Seller" means a seller of alcohol or tobacco products at a retail outlet, or the seller of alcohol or tobacco at a social establishment.[316]
(5) "Permittee" means an owner or agent or employee of an owner who owns a social establishment who checks for proof of age and allows admittance to a social establishment that requires the patron to be of a certain age for entrance.
(6) "Transaction scan" means by which a seller/permittee or an agent or employee of a seller/permittee checks, by means of a transaction scan device, the validity of a driver's license, commercial driver's license, or identification card that is presented as a condition to purchasing alcohol, tobacco, or gaining entrance to a social establishment that sells alcohol or tobacco.[317]
(7) "Transaction scan device" means any commercial device or combination of devices used at a point of sale, or a point of entrance to a social establishment, that is capable of deciphering in an electronically readable format the information encoded on the magnetic strip, bar code, computer chip, or some other type of electronic storage mechanism of a driver's license, commercial driver's license, or identification card.[318]
(8) "Fair information practice principles" means the five core principles as defined in the Federal Trade Commission's 1998 report to Congress and includes (1) notice/awareness, (2) choice/consent, (3) access/participation, (4) integrity/security, (5) enforcement/redress regulating the collection of personal information from the public.[319]
(b)(1) A seller/permittee or an agent or employee of a seller/permittee may perform a transaction scan by means of a transaction scan device to check the validity of a driver's license, commercial driver's license, or identification card presented by a card holder as a condition to selling, giving away, or otherwise distributing alcohol, cigarettes, or other tobacco products.[320]
(2) A seller/permittee or an agent or employee of a seller/permittee may perform a transaction scan by means of a transaction scan device to check the validity of a driver's license, commercial driver's license, or

313. Ohio Rev. Code Ann. § 2927.021; Conn. Gen. Stat. § 30-86.
314. *See generally* at § Ohio Rev. Code Ann. 2927.021 (giving the original statute).
315. *See generally Id.* (giving the original statute).
316. *See Id.* (giving the original statute).
317. *See Id.* (giving the original statute).
318. *See Id.* (giving the original statute).
319. *FTC Report, supra* n. 6, at III.
320. Ohio Rev. Code Ann. § 2927.021; Conn. Gen. Stat. § 30-86.

identification card presented by a cardholder as a condition to gaining admittance to a social establishment.

(3) If the information deciphered by the transaction scan under subdivision (1) or (2) of this subsection fails to match the information printed on the driver's license, commercial driver's license, or identity card presented by the cardholder, or if the transaction scan indicates that the information so printed is false or fraudulent neither the seller/permittee nor any agent of the seller/permittee shall sell, give away, or otherwise distribute any alcohol or tobacco products or allow the card holder to gain admittance to a social establishment.[321]

(4) Division b(1)-(2) of this section does not preclude a seller/permittee or an agent or employee of a seller/permittee from using a transaction scan device to check the validity of a document other than a driver's license, commercial driver's license, or identification card, if the document includes a bar code or magnetic strip that may be scanned by the device, as a condition for selling, giving away, or otherwise distributing alcohol, cigarettes, or other tobacco products to the person presenting the document, or as a condition for admittance to a social establishment to the person presenting the document.[322]

(c)(1) No seller/permittee or agent or employee of a seller/permittee shall electronically or mechanically record or maintain any information derived from a transaction scan, except the following:[323]

(A) The name and date of birth of the person listed on the driver's license, commercial driver's license, or identification card presented by the card holder;[324]

(B) The expiration date and identification number of the driver's license, commercial driver's license, or identification card presented by the cardholder.[325]

(2) No seller/permittee or agent or employee of a seller/permittee shall use a transaction scan device for a purpose other than the purpose specified in divisions b(1)-(2) of this section.[326]

(3) No seller/permittee or agent or employee of a seller/permitee shall sell or otherwise disseminate the information derived from a transaction scan to any third party for any purpose, including, but not limited to, any marketing, advertising, or promotional activities, except that a seller/permittee or agent or employee of a seller/permittee may release that information pursuant to a court order.[327]

(4) Nothing in subsection (b) of this section or this subsection relieves a seller or permittee or agent or employee of a seller or permittee of any responsibility to comply with any other applicable state or federal laws

321. Ohio Rev. Code Ann. § 2927.021; Conn. Gen. Stat. § 30-86.
322. Ohio Rev. Code Ann. § 2927.021; Conn. Gen. Stat. § 30-86.
323. Ohio Rev. Code Ann. § 2927.021; Conn. Gen. Stat. § 30-86.
324. Ohio Rev. Code Ann. § 2927.021.
325. *Id.* at § 2927.021.
326. *Id.* at § 2927.021.
327. Conn. Gen. Stat. § 30-86.

or rules governing the sale, giving away, other distribution of alcohol or tobacco, or gaining admittance to a social establishment.[328]

(d)(1) In any prosecution of a seller/permittee or agent or employee of a seller/permittee for selling, giving away, or otherwise distributing alcohol or tobacco to a legally underage person, or allowing admittance to a social establishment that sells, gives away, or otherwise distributes alcohol or tobacco to a legally underage person, it shall be an affirmative defense that all of the following occurred:[329]

(A) A cardholder attempting to purchase alcohol, tobacco, or gain entry to a social establishment that sells, gives away, or otherwise distributes alcohol or tobacco presented a driver's license, commercial driver's license, or identification card;[330]

(B) a transaction scan of the driver's license, commercial driver's license, or identification card that the card holder presented indicated that the license or card was valid;[331]

(C) the alcohol or tobacco sold, given away, or otherwise distributed or the admittance to the social establishment was approved in reasonable reliance upon the identification presented and the completed transaction scan.[332]

(2) In determining whether a seller/permittee or agent or employee of a seller/permittee has proven the affirmative defense provided by subsection (1) of this subsection, the trier of fact in such prosecution shall consider that reasonable reliance upon the identification presented and the completed transaction scan may require a seller/permittee or agent or employee of a seller/permittee to exercise reasonable diligence and that the use of a transaction scan device does not excuse a seller/permittee or agent or employee of a seller/permittee from exercising such reasonable diligence to determine the following:[333]

(A) Whether a person whom the seller/permittee or an agent or employee of the seller/permittee sells, gives away, or otherwise distributes alcoholic liquor to is of legal age in the respective state to purchase such alcoholic liquor or is of legal age to gain admittance to a social establishment.[334]

(B) Whether a person whom the seller/permittee or an agent or employee of the seller/permittee sells, gives away, or otherwise distributes tobacco is of legal age in the respective state to purchase such tobacco or gain admittance to a social establishment.[335]

(C) Whether the picture appearing on the driver's license or identity card presented by a cardholder is that of the cardholder.[336]

---

328. *Id.* at § 30-86.
329. *Id.* at § 30-86(e).
330. *Id.* at § 30-86(e)(1)(A).
331. *Id.* at § 30-86(e)(1)(B).
332. Conn. Gen. Stat. § 30-86(e)(1)(C).
333. *Id.* at § 30-86(e)(1)(C).
334. Ohio Rev. Code Ann. § 2927.022(B)(1); Conn. Gen. Stat. § 30-86(e)(2)(A).
335. Ohio Rev. Code Ann. § 2927.022(B)(1); Conn. Gen. Stat. § 30-86(e)(2)(A).
336. Ohio Rev. Code Ann. § 2927.022(B)(2); Conn. Gen. Stat. § 30-86(e)(2)(B).

(e)(1) Any transaction scan performed in conjunction with subsection (b) and any data retention performed with subsection (c) shall conform with the fair information practice principles.[337]
(f)(1) Any violation of the data collection and storage process outline in subsection (c) or with the proper collection of data under subsection (e) shall result in a punishment of a fine, and/or a suspension of the business's license, and/or incarceration. The punishment shall be in accordance with the number of offenses committed and the seriousness of the offense. Empowers State Attorneys General to enforce this Act.[338] Establishes Federal injunctive authority regarding any violation of the Act.[339]

A Statutory regulation similar to this will help protect the people's privacy to the utmost degree. America's privacy must be highly protected so people do not fear that taking part in legal transactions could jeopardize their security and safety. A society that fears taking part in certain transactions that are legal could decrease the United States' economy because people may refrain from purchasing items or visiting certain establishments in order to protect their privacy. A person should be able to buy a bottle of wine or go to a club to hear their favorite band without having to exchange their life history for it. The scanning technology is spreading rapidly; the states are haphazardly regulating it, so the federal government should step forward with legislation to curtail scanning before the practice becomes completely uncontrollable.

IV. CONCLUSION

Scanning or swiping of drivers licenses and identification cards to verify age is a practice that has emerged recently because of the development of better technology, and it is ever increasing.[340] Few states have enacted legislation to regulate it, and the federal government has not addressed the issue. Meanwhile, many patrons' private and sensitive information is being stolen by businesses without the customers' knowledge. Federal legislation should be enacted to nationally regulate the practice before a customer becomes the victim of a violent crime, or of an identity theft, which is committed using the patron's stolen personal information. The information included on drivers licenses and identification cards currently is too sensitive for private industry to possess. Additionally there is no valid reason for them to have it. Unaccountable private individuals cannot be entrusted with the duty to protect the security and privacy of hundreds or thousands of people. The federal government has already addressed similar concerns in private industries, in

337. *FTC Report*, *supra* n. 6, at III.
338. Sen. 116, 109th Cong.
339. *Id.*
340. Chung, *supra* n. 1 at 443.

the health care industry with the implementation of HIPAA[341] and with DMVs under the DPPA,[342] and needs to address theses concerns currently with swiping. The owner of a club in New Orleans, who scans identification cards and stores the data, summed up the situation best: "Will I use it [the information scanned from the license] in the wrong way? No. But then again, what is to stop the next guy?"[343] The only way to stop the "next guy" is to regulate scanning and subsequent data retention.

John T. Cross†

341. 42 U.S.C. § 300gg-41 (2004).

342. 18 U.S.C. § 2721.

343. Lee, *supra* n. 1 [¶ 38-39].

† June 2006 graduate of The John Marshall Law School, J.D.; B.S. in Marketing, Southern Illinois University at Carbondale. The author would like to thank everyone whose hard work went into producing this article. Special thanks go out to David Babaian and Reneé Germaine for all of their assistance and guidance throughout the writing and shaping of the article. Finally, thanks go out to my family and Casie for their encouragement and support.