UNC SCHOOL OF LAW

NORTH CAROLINA BANKING INSTITUTE

Volume 11 | Issue 1 Article 13

2007

Scanning Legislative Efforts: Current RFID Legislation Suffers from Misguided Fears

Kristina M. Willingham

Scanning Legislative Efforts: Current RFID Legislation Suffers from Misguided Fears

I. INTRODUCTION

A customer walks into a store, selects an item from a shelf, pockets the item, walks right past the long checkout lines and out the door without stopping, all within a matter of seconds. This may seem like shoplifting, but a lawful transaction may have occurred if the issuer of the customer's credit or debit card and the store use radio frequency identification (RFID).[1] In addition to allowing issuers of debit or credit cards to offer this scenario to their customers as a reality, RFID has the potential to transform and improve the way many financial institutions conduct business.[2] However, many states have introduced legislation that could prevent financial institutions and consumers from fully realizing the benefits of the technology.[3] Since much of the legislation reflects exaggerated fears about RFID, increased awareness and education about the technology is necessary in order to allay these fears and allow financial institutions the opportunity to implement this cost-saving technology.[4]

---

1. *See* Ariana-Michele Moore, *Replacing Cash with Convenience: The Promise of RFID Payments*, BANK SYSTEMS & TECH., Sept. 2, 2003, http://www.banktech.com/showArticle.jhtml?articleID=14700510.

2. *See Riding the Wave of the Future: NCR Demonstrates RFID for Branch Banking*, BUS. WIRE, Oct. 11, 2006.

3. *See* Peter Piazza, *A Chip Off the Privacy Block?*, SECURITY MGMT., July 1, 2006, at 62(7). In 2006, 18 states introduced legislation concerning RFID. 2006 Privacy Legislation Related to Radio Frequency Identification (RFID), Nat'l Conf. of State Legislatures, http://www.ncsl.org/programs/lis/privacy/rfid06.htm [hereinafter 2006 Privacy Legislation] (last visited Feb. 3, 2007). These states included Ala., Cal., Fla., Ga., Ill., Kan., Mass., Mich., Mo., N.H., N.J., N.Y., Ohio, Okla., R.I., Tenn., Wash., and Wis. *Id.* In 2005, 16 states introduced legislation concerning RFID. 2005 Privacy Legislation Related to Radio Frequency Identification (RFID), Nat'l Conf. of State Legislatures, http://www.ncsl.org/programs/lis/privacy/rfid05.htm [hereinafter 2005 Privacy Legislation] (last visited Feb. 3, 2007). These states included Cal., Ill., Md., Mass., Mo., Nev., N.H., N.M., R.I., S.D., Tenn., Tex., Utah, Va., Wis., and Wyo. *Id.*

4. *See* Nicholas Evans, *RFID-Enabled IDs: Educate, Don't Legislate*, RFID J., Aug. 28, 2006, http://www.rfidjournal.com/article/articleview/2615/1/82/.

RFID is a technological tool to identify people or objects using radio waves.[5] Information, such as a person's credit account information or an object's price, is digitally stored on an RFID tag.[6] When an RFID tag comes within range of an RFID reader, the RFID tag sends electromagnetic waves to the RFID reader.[7] The RFID reader then converts these electromagnetic waves into digital data which can then be passed on to a computer.[8]

RFID is not a new technology.[9] In fact, thousands of companies already use RFID.[10] Currently, RFID is most commonly used for controlling access to buildings and parking garages, tracking inventory, paying highway tolls, and purchasing gasoline.[11] RFID is now getting more attention, however, because more businesses, including financial institutions, are seeking to

---

5. RFID Journal, What is RFID?, http://www.rfidjournal.com/faq/16/49 (last visited Feb. 3, 2007).

6. *See id.* There are three types of RFID tags: passive, active, and semi-passive. *See* RFID Journal, What's the Difference Between Passive and Active Tags?, http://www.rfidjournal.com/faq/18/68 (last visited Feb. 3, 2007). Passive RFID tags consist of a microchip that is attached to an antenna. What is RFID?, *supra* note 5. When the passive RFID tag comes within range of an RFID reader, the passive RFID tag receives electromagnetic waves emitted by the RFID reader. RFID Journal, How Does an RFID System Work?, http://www.rfidjournal.com/faq/17/58 (last visited Feb. 3, 2007). These electromagnetic waves power the passive RFID tag, which then sends electromagnetic waves back to the RFID reader. *Id.* Active RFID tags, on the other hand, have a battery or other power source and thus are not powered by the RFID reader. What's the Difference Between Passive and Active Tags?, *supra*. As a result, active RFID tags continuously transmit electromagnetic waves, whether in range of an RFID reader or not. *Id.* When an active RFID tag comes within range of an RFID reader, the RFID reader receives the electromagnetic waves from the active RFID tag and converts them into digital data. *Id.* Semi-passive RFID tags are battery-powered like active RFID tags but only transmit electromagnetic waves when within range of an RFID reader like passive RFID tags. *Id.* Passive RFID tags work best when the tag and the reader are in close proximity. MoreRFID, What is the Difference Between a Passive, Semi-passive and Active RFID?, http://www.morerfid.com/index.php?do=faq&topic=Introduction-8&display=RFID (last visited Feb. 3, 2007). Active and semi-passive RFID tags, on the other hand, can be scanned from much longer ranges. What's the Difference Between Passive and Active Tags?, *supra*.

7. How Does an RFID System Work?, *supra* note 6.

8. *Id.*

9. RFID Journal, Is RFID New?, http://www.rfidjournal.com/faq/16/52 (last visited Feb. 3, 2007) ("RFID is a proven technology that's been around since at least the 1970s.").

10. RFID Journal, Are Any Companies Using RFID Today?, http://www.rfidjournal.com/faq/16/55 (last visited Feb. 3, 2007).

11. RFID Journal, What Are Some of the Most Common Applications for RFID?, http://www.rfidjournal.com/faq/16/56 (last visited Feb. 3, 2007).

implement it in ways that will affect most consumers.[12] American Express, Visa, and MasterCard have already launched pilot programs to test RFID and customer reaction to it.[13] Visa is also currently issuing RFID-tagged prepaid cards that can be used anywhere that has an open network payment system and accepts RFID payments.[14]

This Note explains why education and awareness of RFID are essential if financial institutions are to benefit from the technology. In Part II, this Note outlines the benefits of RFID to financial institutions.[15] Part III examines the drawbacks that financial institutions may face in attempting to implement an RFID system.[16] Part IV explores potential ways for financial institutions to overcome these drawbacks.[17] Part V evaluates the current legislation concerning RFID and explains why it needlessly inhibits use and expansion of RFID.[18] Part VI of this Note analyzes how education and increased awareness can help allay the fears that have driven much of the current RFID legislation.[19]

II. POTENTIAL BENEFITS OF RFID

A. *More Personalized Service to Customers*

The financial industry can greatly benefit from RFID.[20] For example, a depository institution could embed RFID tags in its customers' existing cards and place an RFID reader near the entrance.[21] When the customer enters the depository institution

12. *See* Daniel Sieberg, *Is RFID Tracking You?*, CNN.COM, Oct. 23, 2006, http://www.cnn.com/2006/TECH/07/10/rfid/index.html.

13. Moore, *supra* note 1.

14. David Breitkopf, *Visa Puts Prepaid Contactless Cards on Open Network*, AM. BANKER, Dec. 14, 2006, at 18. An open network is a "network implemented to an industry-accepted standard." Satellite Retailers Glossary, http://www.satelliteretailers.com/glossary.html#o (last visited Feb. 3, 2007).

15. *See infra* notes 20-46 and accompanying text.

16. *See infra* notes 47-71 and accompanying text.

17. *See infra* notes 72-103 and accompanying text.

18. *See infra* notes 104-81 and accompanying text.

19. *See infra* notes 182-218 and accompanying text.

20. *See, e.g.*, *RFID May Boost Service at Banks*, RFID J., Apr. 25, 2003, http://www.rfidjournal.com/article/articleview/396/1/1/.

21. *Id.*; Elizabeth Wasserman, *Cashing in on RFID's Benefits*, RFID J., http://www.rfidjournal.com/magazine/article/2590/1/373/ (last visited Feb. 3, 2007).

carrying the card, the RFID reader could scan the RFID tag in the card and send the customer's information to the teller.[22] Before the customer has reached the teller's window, the teller could know the customer's name, preferences, account balances, and recent transactions, as well as whether the customer is an elite customer requiring special attention.[23] The result is more personalized service since customers can be greeted by name before they have approached the teller, and the teller will be able to quickly deliver service that is tailored to customers' individual preferences.[24] Moreover, the RFID system could alert a manager to the presence of any elite customers so that such customers can receive the benefits of their elite status, which could include avoiding a long wait in line and receiving extra attention.[25] Further, a depository institution could make use of RFID in order to market its financial products in an exceptionally timely manner.[26] For example, if a depository institution's customer has a certificate of deposit that is about to mature, the RFID system could notify the teller to discuss reinvestment options with the customer.[27]

B. Document- and Information-Tracking

Financial institutions record sensitive information such as bank accounts, credit card transactions, and loan applications on data tapes.[28] Loss of these data tapes can negatively impact the financial institution's financial condition and reputation.[29]

---

22. *RFID May Boost Service at Banks*, *supra* note 20.

23. *Id.*

24. *Id.*; Wasserman, *supra* note 21. "The trade-off would be similar to a customer's decision to use a supermarket loyalty card;" the customer would allow the bank to gather information about the customer in exchange for the customer receiving faster and more personalized service. *Id.*

25. Wasserman, *supra* note 21.

26. *See Riding the Wave of the Future: NCR Demonstrates RFID for Branch Banking*, *supra* note 2.

27. *Id.*

28. Wasserman, *supra* note 21.

29. Sean C. Honeywill, *Data Security and Data Breach Notification for Financial Institutions*, 10 N.C. BANKING INST. 269, 270 (2006); Wasserman, *supra* note 21 (noting that state laws may require a financial institution to notify customers of

Citigroup, ABN Amro, Bank of America, and Peoples Bank have all recently lost data tapes containing the personal information of millions of customers.[30] Data tapes are usually lost during transportation to another facility or when employees remove them from the financial institution's libraries to verify data.[31]

Financial institutions could embed RFID tags in these data tapes and in employee identification cards and place an RFID reader in the rooms housing the sensitive documents.[32] This RFID system would enable a financial institution to keep records of when and by whom data tapes are removed from the storage facility.[33] The RFID reader could also alert a security official in real-time if an unauthorized party removed or attempted to remove a data tape.[34] When transporting data tapes, the financial institution could place an RFID reader in the transportation vehicle so that the financial institution could track the location of the data tapes in real-time.[35] In addition to tracking data tapes, financial institutions could use RFID to track other valuables, including bags of currency, cancelled checks, bearer bonds, and security documents.[36]

C. *Increased Convenience for Customers*

Although RFID payment programs were originally designed to replace cash, issuers of debit and credit cards are now developing RFID payment programs as an alternative to payments with debit and credit cards.[37] The mechanism behind this alternative payment program consists of creating a link between an

---

potential privacy breaches when data tapes are lost and the estimated cost to the financial institution is $1 per notification letter).

30. Wasserman, *supra* note 21.

31. *Id.*

32. *See* Paul Kallender, *Japanese Bank Taps NEC for Document Security Using RFID*, COMPUTERWORLD, Aug. 18, 2004, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=95327&pageNumber=1.

33. *Id.*

34. *Id.*

35. Wasserman, *supra* note 21.

36. *Id.*

37. Moore, *supra* note 1. RFID payments are also referred to as "contactless payments." *Id.*

RFID tag and a customer's debit, credit, or prepaid account so that the customer could use the RFID tag to make purchases.[38] Because RFID tags are small, they may be embedded in key chains or mobile phones,[39] thereby eliminating the need for a customer to carry cash or even a wallet in many situations.[40] When making purchases, the customer could simply hold the RFID-tagged payment device close to an RFID reader in lieu of swiping a debit or credit card.[41] The payment would then be processed in the same manner as a debit or credit transaction, with the customer entering a personal identification number (PIN) or signing a receipt if required.[42] The result is a reduced transaction time compared to payments by cash or magnetic stripe cards.[43]

The potential for an even shorter transaction time exists if the product being purchased contains an RFID chip as well, as illustrated in the beginning of this Note.[44] A customer could potentially fill a shopping cart with goods, walk through a tunnel RFID reader which would automatically read and price the goods still in the cart, and pay with the swipe of an RFID key chain, mobile phone, or card.[45] Thus, RFID allows issuers of debit and credit cards to offer customers more convenience and quicker service, which in turn could attract new customers and increase loyalty among existing customers.[46]

---

38. Mary Catherine O'Connor, *Chase Offers Contactless Cards in a Blink*, RFID J., May 24, 2005, http://www.rfidjournal.com/article/articleview/1615.

39. Moore, *supra* note 1.

40. *See* Jay MacDonald, *Paying by Cell Phone on the Way*, BANKRATE.COM, Mar. 28, 2005, http://www.bankrate.com/brm/news/cc/20050329a1.asp.

41. *See* O'Connor, *supra* note 38.

42. *Id.*

43. Mary Catherine O'Connor, *Accelitec Unveils RFID Payment System*, RFID J., Aug. 17, 2005, http://www.rfidjournal.com/article/articleview/1811/1/1/; *see also* Robin Hohman, *Contactless Cards: Are Privacy Jitters Legit?*, TECHNEWSWORLD, Sept. 28, 2006, http://www.technewsworld.com/story/53273.html ("Consumers conducting transactions with [RFID cards] were able to conduct transactions fifty-three to sixty-three percent faster than with cash . . . ."); O'Connor, *supra* note 38 ("Pilot programs have found as much as a twenty-second reduction in transaction time using [RFID] payments . . . .").

44. *RFID Business Applications*, RFID J., http://www.rfidjournal.com/article/articleview/1334/1/129/ (last visited Feb. 3, 2007).

45. *See id.*; Ken Spencer Brown, *Cutting-Edge Systems Streamline Shopping*, INVESTOR'S BUS. DAILY, July 17, 2006, at A10.

46. Jeffrey Noe, *Contactless Cards: The Next Big Thing?*, ABA BANKING J., Sept. 2005, at 42.

III. POTENTIAL DRAWBACKS OF RFID

A. *Risk of Viruses*

RFID systems may be vulnerable to a virus attack.[47] Although RFID tags generally contain little memory, it took a student at a university in the Netherlands only four hours to write a virus small enough to fit on an RFID tag.[48] When a virus is embedded in an RFID tag, that virus could potentially infect the financial institution through the financial institution's RFID reader.[49] Such viruses would not only damage a financial institution's computer system but also allow the hacker to use or alter any data stored on the computer system.[50] Given the substantial risk that viruses pose to RFID systems, the technology is useless and potentially damaging to financial institutions if such systems cannot be protected from viruses.[51]

B. *Data Security*

Researchers at Johns Hopkins University demonstrated that for a few hundred dollars, a thief could purchase the equipment necessary to steal data from an RFID tag, "crack" the encryption key on the RFID tag, and then clone the RFID tag.[52] According to the Johns Hopkins researchers, this task could be accomplished using a device as small as an Apple iPod, which suggests that it could be easily concealed.[53] The small device functions both as an RFID reader and RFID tag by reading data from the targeted RFID tag and then serving as a clone of that

47. Jeremy Kirk, *RFID Tags Vulnerable to Viruses*, COMPUTERWORLD, Mar. 15, 2006, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=109560.

48. *Id.*

49. *Id.*

50. *Id.*

51. *See id.*

52. STEVE BONO ET AL., JOHNS HOPKINS UNIV. INFO. SEC. INST., SECURITY ANALYSIS OF A CRYPTOGRAPHICALLY-ENABLED RFID DEVICE 2 (2005), *available at* http://rfidanalysis.org/DSTbreak.pdf.

53. *Id.* at 4.

tag.[54] Reading the data would not require contact with the RFID tag or with the consumer carrying the RFID tag.[55] The thief would simply need to be in close proximity to the RFID tag.[56] Therefore, even if an RFID tag never left the hands of the consumer, the information contained on that RFID tag could be used by a third party to make purchases from the consumer's account.[57] If the data contained on RFID tags cannot be protected from hackers, the risk of fraud is likely too great for financial institutions to consider using RFID.[58]

C. *Customer Privacy*

Some critics of RFID are concerned that use of RFID tags could lead to a "Big Brother" scenario wherein every movement and every purchase made by a customer carrying an RFID tag could be tracked, not only by the entity issuing the RFID tag, but also by any individual or entity utilizing an RFID reader.[59] These critics fear that without customer consent or knowledge, a merchant could potentially create a log of each customer's past purchases and then sell or share this information with other businesses.[60] In order to assuage this fear, depository institutions and issuers of debit and credit cards will need to demonstrate a commitment to protecting customer privacy and show that they are taking precautions to ensure that customer privacy will not be

54. *Id.* at 2.

55. *See id.* at 4.

56. *Id.* If the RFID tag was passive, the individual would simply need to be within a few inches of the RFID tag for a fraction of a second. Ari Juels, *Attack on a Cryptographic RFID Device*, RFID J., Feb. 28, 2005, http://www.rfidjournal.com /article/articleview/1415/1/39/. If the RFID tag was active or semi-passive, the individuals would not even need to be that close in order to steal the information. *Id.*

57. BONO ET AL., *supra* note 52, at 4.

58. *See* Juels, *supra* note 56.

59. *See* Jay Cline, *The RFID Privacy Scare is Overblown*, COMPUTERWORLD, Mar. 15, 2004, http://www.computerworld.com/securitytopics/security/story/0,10801, 91125,00.html; Rich McIver, *RFID Privacy Issues*, RFID GAZETTE, Mar. 22, 2005, http://www.rfidgazette.org/2005/03/rfid_privacy_is.html. An individual or entity needs only a few hundred dollars and some technological savvy in order to fashion an RFID reader, but tracking an individual's movements is not feasible with just one RFID reader and tracking an individual's purchases is not feasible unless the RFID reader is in close proximity to the targeted RFID tag. *See* Juels, *supra* note 56.

60. McIver, *supra* note 59.

compromised.[61] Additionally, financial institutions employing RFID can stress that their use of RFID will have to comply with existing rules and regulations protecting customer privacy.[62] If these financial institutions cannot overcome privacy concerns, their customers will not embrace or utilize the technology, and attempts to increase customer satisfaction and profits through the use of RFID will fail.[63]

D. Cost

Use of RFID systems on a mass scale can be costly.[64] In addition to initial startup costs,[65] the cost to a financial institution of a single RFID tag ranges from twenty cents to six dollars depending on the intended application and the volume ordered,[66] while the cost of an RFID reader ranges from $1,000 to $3,000.[67] The RFID industry anticipates that the cost of a single RFID tag will drop as low as five cents, however, if the technology is adopted by more businesses.[68] Increased use of RFID by financial institutions will therefore help to lower the cost.[69] However, if the decrease in cost is insufficient, other businesses are unlikely to find RFID cost-effective and will not implement it.[70] Without many businesses equipped to accept RFID payments, issuers of debit

61. *See* Piazza, *supra* note 3 ("[A]ny company that uses RFID needs to take the privacy principles to heart if it hopes to win, and keep, customer support.").

62. *See infra* notes 209-18 and accompanying text.

63. *See* Piazza, *supra* note 3.

64. RFID Journal, What Has Prevented RFID From Taking Off Until Now?, http://www.rfidjournal.com/faq/16/54 (last visited Feb. 3, 2007).

65. *See* RFID Journal, How Much Does a Fully Functional RFID System Cost?, http://www.rfidjournal.com/faq/20/87 (last visited Feb. 3, 2007) (noting that startup costs may include infrastructure costs, personnel training, installation costs, and network upgrading costs). Because these costs depend on too many factors, it is not possible to give an accurate estimate of the startup costs to a financial institution. *Id.*

66. RFID Journal, How Much Does an RFID Tag Cost Today?, http://www.rfidjournal.com/faq/20/85 (last visited Feb. 3, 2007).

67. RFID Journal, How Much Do RFID Readers Cost Today?, http://www.rfidjournal.com/faq/20/86 (last visited Feb. 3, 2007).

68. RFID Journal, Can I Buy a 5-Cent RFID Tag?, http://www.rfidjournal.com/faq/20/84 (last visited Feb. 3, 2007).

69. *See id.*

70. *See* RFID Journal, If RFID Has Been Around So Long and Is So Great, Why Aren't All Companies Using It?, http://www.rfidjournal.com/faq/16/53 (last visited Feb. 3, 2007).

and credit cards will not be able to use RFID for payment systems.[71]

IV. HOW TO OVERCOME THE POTENTIAL DRAWBACKS OF RFID

A. *A Well Designed RFID System Reduces the Virus Risk*

A well designed RFID system would protect a financial institution from potential viruses.[72] A virus would only be able to infect an RFID system if the system treated the data contained on an RFID tag as executable code.[73] Only a poorly designed RFID system, however, would treat the data as such.[74] A well designed RFID system would treat the data simply as data to be read rather than as instructions to be executed.[75] Thus, if a financial institution implements a well designed RFID system, the risk of a virus infection is low.[76]

B. *Overcoming Security and Privacy Concerns*

1. Encrypted Data May Increase Security

The data contained on an RFID tag can be, and usually is, encrypted for security purposes.[77] Researchers at Johns Hopkins were successful in stealing and cloning the RFID tag only because they were able to "crack" the tag's forty-bit encryption key.[78] One solution the researchers themselves proposed is that RFID tags

---

71. *See MasterCard to Test RFID Card*, RFID J., Dec. 20, 2002, http://www.rfidjournal.com/article/articleview/171/1/1/.

72. *See The Industry Reacts to RFID Virus Research*, RFID UPDATE, Mar. 20, 2006, http://www.rfidupdate.com/articles/index.php?id=1077; John Walko, *Experts Refute RFID Virus Claims*, BANK SYSTEMS & TECH., Mar. 17, 2006, http://www.banktech.com/aml/showArticle.jhtml?articleID=183701403&pgno=1.

73. *The Industry Reacts to RFID Virus Research*, *supra* note 72 ("For an RFID system to interpret tag data [as code] would require a poor, insecure design that breaks the most basic and obvious rules of system engineering.").

74. *Id.*

75. Walko, *supra* note 72.

76. *The Industry Reacts to RFID Virus Research, supra* note 72.

77. Sieberg, *supra* note 12.

78. BONO ET AL., *supra* note 52, at 2; *see supra* notes 52-58 and accompanying text.

should contain a 128-bit key instead of a forty-bit key.[79] A 128-bit key would effectively render the data contained on the RFID tag useless to a thief because today's computers are not capable of "cracking" 128-bit keys within a customer's lifetime.[80] A longer encryption key, however, could substantially increase the cost of RFID tags and reduce customer transaction speeds.[81] As such, financial institutions should carefully examine the potential benefits of RFID technology in order to decide whether the costs of this increased security measure would make an RFID system worthwhile.[82]

2. Radio-Reflective Shielding May Increase Security and Protect Customer Privacy

In order to prevent customers' RFID tags from being read without their consent or knowledge, depository institutions and issuers of debit and credit cards may consider providing their customers with an aluminum foil case or other radio-reflective shield in which to carry their RFID tags when not in use.[83] Radio waves bounce off metal, so a radio-reflective shield would provide security by thwarting efforts by would-be thieves to steal the data contained on an RFID tag.[84] In addition, such shields would protect customers' privacy by preventing anyone from tracking an

79. BONO ET AL., *supra* note 52, at 5.

80. *See* LORRAINE C. WILLIAMS, SANS INST., A DISCUSSION OF THE IMPORTANCE OF KEY LENGTH IN SYMMETRIC AND ASYMMETRIC CRYPTOGRAPHY 3, *available at* http://www.giac.org/certified_professionals/practicals/gsec/0848.php; Evan Schuman, *How Safe Are the New Contactless Payment Systems?* CIO INSIGHT.COM, June 20, 2005, http://www.cioinsight.com/print_article2/0,2533,a=154404,00.asp. A 128-bit encryption key simply means that 128-bits are used to encrypt the message contained on the RFID tag. WILLIAMS, *supra*. The longer the encryption key, the harder it is to crack. *Id.* at 1. A 128-bit encryption key would take 5.4×10^{10} years for today's computers to "crack." *Id.* at 3. "[A] 128-bit [encryption] key[] should be safe for [fifty] years at least." *Id.*

81. BONO ET AL., *supra* note 52, at 5; John Schwartz, *Researchers See Privacy Pitfalls in No-Swipe Credit Cards*, N.Y. TIMES, Oct. 23, 2006, at C1.

82. *See* Schwartz, *supra* note 81.

83. BONO ET AL., *supra* note 52, at 5.

84. RFID Journal, I've Heard That RFID Doesn't Work Around Metal and Water. Does That Mean I Can't Use It to Track Cans or Liquid Products?, http://www.rfidjournal.com/faq/18/73 (last visited Feb. 3, 2007).

RFID tag as long as it is housed in a shield.[85] Ensuring that an RFID tag is always encased in a radio-reflective shield presents an inconvenience, however, that would be magnified if the RFID tag was embedded in a frequently used device such as a mobile phone or key chain.[86] Additionally, if customers always keep their RFID tags encased in radio-reflective shields, depository institutions would not be able to use RFID to provide more personalized customer service.[87]

3. RFID Tags with an On/Off Switch May Increase Security and Protect Customer Privacy

Financial institutions using RFID may wish to fit all of their RFID tags with an on/off switch.[88] An RFID tag with an on/off switch only transmits or receives electromagnetic waves when the customer has the tag "turned on."[89] This feature would boost the security of tags by preventing thieves from stealing the data from the RFID tag remotely.[90] The tag itself would still be vulnerable to theft, but this vulnerability is no different than that of a debit or credit card. Such tags would also protect customer privacy by preventing anyone from tracking the RFID tag unless the tag was turned on.[91] RFID tags with this feature, however, are more expensive.[92] Additionally, like radio-reflective shields, if RFID tags

85. *See* Geeta Dayal, *QuickStudy: Faraday Cages*, COMPUTERWORLD, Aug. 23, 2006, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9002661&pageNumber=2.

86. *See* BONO ET AL., *supra* note 52, at 5.

87. *Cf.* Dayal, *supra* note 85 (noting that radio reflective shields would prevent RFID systems from reading information contained on any RFID-tagged card).

88. Prasad Paturi, *Switching Off Credit Card Fraud*, RFID J., Sept. 12, 2005, http://www.rfidjournal.com/article/articleview/1843/1/82/.

89. *See id.* An RFID tag could be fitted with a switch that, for passive RFID tags, would make or break the connection between the chip and antenna and, for active RFID tags, would turn off the battery or power source. *Id.* To "turn on" the RFID tag, the customer would simply squeeze the switch. *Id.*

90. *See id.*

91. *See id.* ("[An on/off switch] ensur[es] no data is captured from the card . . . without the notice and permission of the owner.").

92. *See* Paturi, *supra* note 88.

are fitted with on/off switches, depository institutions would not be able to use RFID to provide more personalized customer service.[93]

4. Increased Use and Transferring Costs to Customers May Make RFID More Accessible for More Businesses

RFID systems are currently too costly for widespread use by most businesses, but as demand for and use of the technology increases, the price is expected to drop.[94] Merchants that currently accept debit and credit cards as forms of payment already have the infrastructure to implement an RFID payment system.[95] Thus, if more of these merchants start using RFID systems or expand their current use of these systems, the cost is expected to fall to the point where businesses can use RFID on a mass scale.[96] To facilitate increased use in the meantime, issuers of debit and credit cards could reduce or eliminate the merchant fees for payments using RFID until the merchant has recovered the cost of the RFID readers.[97] Although reducing or eliminating merchant fees will add to the issuer's initial costs of implementing an RFID system, such a promotional maneuver could lower the long-term costs of the technology.[98]

Financial institutions may choose to pass on certain RFID costs partially or totally to their customers.[99] For example, if an issuer of debit or credit cards implements a more expensive but safer feature such as an on/off switch or a longer encryption key, it

---

93. *Cf. id.* (noting that an RFID system cannot read the information contained on an RFID tag if the tag is off).

94. *See Chain Reactions*, ECONOMIST, June 17, 2006. The RFID industry hopes to increase use of the technology to the point where an RFID tag costs only five cents. Can I Buy a 5-Cent RFID Tag?, *supra* note 68.

95. Noe, *supra* note 46 ("To accelerate market penetration [of RFID], Visa, MasterCard[,] and American Express have all agreed to a common [RFID] communications protocol . . . .").

96. *Chain Reactions*, *supra* note 94.

97. *Cf.* O'Connor, *supra* note 43 ("Major credit card associations and issuing banks are asking retailers to equip their stores with new RFID-enabled payment terminals that will accept RFID payment cards . . . . But the card associations are not lowering transaction fees . . . and merchants aren't happy about that.").

98. *See Chain Reactions*, *supra* note 94 ("If . . . retailers greatly expand their use of RFID tags, the price of each tag will keep falling and mass adoption will move closer.").

99. *See* Paturi, *supra* note 88.

could charge customers a small transaction fee as a way of recouping the costs of the feature.[100] In this way, the customers who benefit from the issuer's use of RFID help pay for some of its costs.[101] However, higher prices could decrease customer interest in the technology,[102] meaning the issuer's attempts to increase customer loyalty and profits through use of RFID will fail.[103]

V. RFID LEGISLATION

To date, the federal government has not enacted legislation to regulate RFID directly.[104] In 2004, the Opt Out of ID Chips Act[105] was introduced in the House of Representatives but died in committee.[106] The Opt Out of ID Chips Act required entities issuing RFID-tagged products to place a warning label on all such products and to give consumers the option of removing or disabling the RFID tag upon issuance.[107] In 2005, the federal government enacted the Real ID Act, which requires that all state

---

100. *Id.*

101. *See id.*

102. *Cf. id.* (noting that RFID issuers will have to pass on the extra cost to consumers and consumers might not be willing to pay a higher amount). Consumers are sensitive to bank fees. *See* FED. RESERVE BD. OF S.F., FRBSF ECON. LETTER NO. 2005-36, at 2 (2005), *available at* http://www.frbsf.org/publications/economics/letter/2005/el2005-36.pdf. One study indicated that increasing an ATM fee by ten cents would result in a four percent decrease in the likelihood of a consumer using that ATM. *Id.*

103. *Cf.* Piazza, *supra* note 3.

104. *See* Laura Hildner, *Defusing the Threat of RFID: Protecting Consumer Privacy Through Technology-Specific Legislation at the State Level*, 41 HARV. C.R.-C.L. L. REV. 133, 151 (2006) ("Industry advocates have substantial support at the federal level in their resistance to RFID-specific legislation."). In a 2004 workshop, Federal Trade Commission (FTC) staff concluded that self-regulation by the RFID industry is sufficient for addressing privacy concerns as long as the self-regulation meets several requirements. STAFF OF THE FED. TRADE COMM'N, RADIO FREQUENCY IDENTIFICATION: APPLICATIONS AND IMPLICATIONS FOR CONSUMERS 22 (2005), *available at* http://www.ftc.gov/os/2005/03/050308rfidrpt.pdf. These requirements include notifying consumers when RFID technology is being used, implementing accountability provisions to ensure that issuing entities are protecting consumers' personal information, and educating consumers about RFID. *Id.* at 22-23. The FTC staff indicated that legislation might be necessary in the future if self-regulation proves insufficient. *Id.* at 23.

105. H.R. 4673, 108th Cong. (2004).

106. Hildner, *supra* note 104. The Opt Out of ID Chips Act has not been reintroduced in Congress. *Id.*

107. H.R. 4673.

drivers' licenses conform to federal standards by 2008.[108] Although the standards outlined in the Real ID Act do not require that drivers' licenses contain RFID, the Real ID Act gives the Secretary of Homeland Security the authority to impose such a requirement in addition to the outlined standards.[109] Some commentators expect that the Secretary will in fact impose this requirement.[110] If this happens, the federal government may then decide to regulate RFID.[111]

State governments, on the other hand, have been much more active in attempting to regulate RFID, with many state legislators hoping that their bills will shape the direction of future federal legislation rather than be preempted by it.[112] Since 2004, RFID legislation has been signed into law in New Hampshire, Utah, Virginia, Wisconsin, and Wyoming.[113] Many other states are currently considering proposed RFID legislation.[114] The only states whose governors have vetoed RFID legislation are Rhode Island and California.[115] Legislation not discussed in this piece

---

108. Real ID Act of 2005, Pub. L. No. 109-13, §§ 201-207, 119 Stat. 231, 311-16 (codified at 49 U.S.C.A. § 30301 note (2005)).

109. *Id.* § 205(a), 119 Stat. at 315 ("All authority to issue regulations, certify standards, and issue grants under this title shall be carried out by the Secretary [of Homeland Security], in consultation with the Secretary of Transportation and the States.").

110. Anita Ramasastry, *Why the 'Real ID' Act Is a Real Mess*, CNN.COM, Aug. 12, 2005, http://www.cnn.com/2005/LAW/08/12/ramasastry.ids/index.html ("In the past, the Department of Homeland Security has indicated it likes the concept of RFID chips.").

111. *See* Letter from Arnold Schwarzenegger, Governor of Cal., to Members of the California State Senate, *available at* http://gov.ca.gov/pdf/press/sb_768_veto.pdf (last visited Feb. 3, 2007).

112. *See, e.g.*, John Leyden, *California Mulls RFID Privacy Law*, THE REG., Sept. 26, 2006, http://www.theregister.co.uk/2006/09/26/california_rfid_law/.

113. *See e.g.*, Assem. 290, 97th Leg., Reg. Sess. (Wis. 2006) (enacted); H.R. 203, 159th Gen. Ct., Reg. Sess. (N.H. 2005) (enacted); H.R. 185, 2005 Leg., Reg. Sess (Utah 2005) (enacted); H.R. 258, 58th Leg., Reg. Sess. (Wyo. 2005) (enacted); S. 148, 2004 Gen. Assem., Reg. Sess. (Va. 2004) (enacted); *see also* 2006 Privacy Legislation, *supra* note 3; 2005 Privacy Legislation, *supra* note 3.

114. *See* 2006 Privacy Legislation, *supra* note 3; 2005 Privacy Legislation, *supra* note 3.

115. *See* H.R. 7432, 2005-2006 Leg., Jan. Sess. (R.I. 2006) (vetoed June 23, 2006); H.R. 5929, 2005-2006 Leg., Jan. Sess. (R.I. 2005) (vetoed July 15, 2005); S. 768, 2005-2006 Leg., Reg. Sess. (Cal. 2005) (vetoed Sept. 30, 2006); *see also* 2006 Privacy Legislation, *supra* note 3; 2005 Privacy Legislation, *supra* note 3. Rhode Island Governor Donald L. Carcieri has vetoed legislation banning state and local governments from tracking individuals because the legislation "is unclear, overly-

includes legislation that creates a group to study the technology and make recommendations on whether further legislation is needed, as well as legislation that criminalizes theft of data from an RFID tag.[116] The remaining RFID legislation tends to fall into one of the following general categories: restrictive, disclosure, or extreme privacy legislation.[117]

A. Restrictive Legislation

The Alabama legislature introduced the Identity Information Protection Act of 2006 (the IIPA),[118] which presents an example of a state effort to impose restrictions and conditions on the use of RFID. This act in many respects mirrors restrictive legislation that was recently vetoed in California.[119] The IIPA mandates several requirements for all identification documents containing RFID tags that are "created, mandated, purchased, or issued by a state, county, or municipal government."[120] One of the requirements is that there must be mutual authentication between the RFID tag and the RFID reader when personal information is

---

broad and could needlessly interfere with many agencies' legitimate responsibilities to properly manage State assets" and to protect the public. Letter from Donald L. Carcieri, Governor of R.I., to The Speaker of the House (July 15, 2005), *available at* http://vote-smart.org/veto_letters/pdf_carcieri_ri_hb5929.pdf; Letter from Donald L. Carcieri, Governor of R.I., to The President of the Senate (June 23, 2006), *available at* http://vote-smart.org/veto_letters/pdf_carcieri_ri_s2768.pdf; Letter from Donald L. Carcieri, Governor of R.I., to The Speaker of the House of Representatives (June 23, 2006), *available at* http://vote-smart.org/veto_letters/pdf_carcieri_ri_h7432.pdf. California Governor Arnold Schwarzenegger has vetoed legislation imposing restrictions and conditions on RFID because it "may impose requirements in California that would contradict the federal mandates soon to be issued" and because of concerns that "the bill's provisions are overbroad and may unduly burden the numerous beneficial new applications of [RFID] technology." Letter from Arnold Schwarzenegger to Members of the California State Senate, *supra* note 111.

116. *See* 2006 Privacy Legislation, *supra* note 3; 2005 Privacy Legislation, *supra* note 3.

117. RFID Law Blog, RFID Legislation: What You Need to Know about the Debate, http://rfidlawblog.mckennalong.com/archives/state-legislation-100-rfid-legislation-what-you-need-to-know-about-the-debate.html (Sept. 20, 2006).

118. S. 310, 2006 Leg., Reg. Sess. (Ala. 2006).

119. *Compare id.*, *with* Cal. S. 768. The California bill differs from the Alabama bill in that the California bill does not recognize radio-reflective shields as acceptable privacy control measures and it does not specify what types of authentication or data encryption are acceptable. *Compare* Ala. S. 310, *with* Cal. S. 768. *See generally supra* text accompanying note 115.

120. Ala. S. 310 § 4(a).

being transmitted.[121] The reason for this requirement is to ensure that the RFID tag's information is only being shared with an authorized reader.[122] Another requirement is that if the RFID tag contains "personally identifiable information," the data must be encrypted.[123] Additionally, the entity issuing the RFID-tagged document must notify the recipient in writing that the document could "be read remotely without his or her knowledge."[124]

The IIPA attempts to give individuals a measure of control over the transmission of the data contained in their RFID tags.[125] The IIPA essentially allows individuals to opt out of having their RFID tags read by requiring the issuing entity to implement one of three possible privacy control measures.[126] One privacy control measure the issuing entity could implement includes installing an "access control protocol" at all locations where the card needs to be used so that the RFID tag could be read without the use of radio waves.[127] This way, individuals could manually swipe their cards through a machine and manually enter a PIN in lieu of allowing their cards to be read by the RFID reader.[128] A second privacy control measure the issuing entity could employ is to fit the RFID tag with an on/off switch that would allow the individual to turn the tag off when not in use.[129] Alternatively, the issuing entity could distribute a radio-reflective shield to all individuals receiving an RFID tag.[130]

While all of these measures protect the privacy of consumers, they may also increase the costs and complicate the use of RFID to the point where the costs outweigh the benefits.[131]

---

121. *Id.* § 4(a)(2). Authentication is "the process of applying a specific mathematical algorithm to data or identification documents, or both." *Id.* § 3(1). Mutual authentication is "the use of authentication to ensure that authorized readers can reliably detect unauthorized identification documents, and that authorized identification documents can be read only by those authorized readers." *Id.* § 3(9).

122. *Id.* § 3(9).

123. *Id.* § 4(a)(3).

124. Ala. S. 310 § 4(a)(5).

125. *See id.* § 4(a)(4).

126. *Id.*

127. *Id.*

128. *See id.*

129. *Id.*; *see supra* Part notes 88-93 and accompanying text.

130. Ala. S. 310 § 4(a)(4).

131. *See* RFID Law Blog, *supra* note 117.

Additionally, if applied to the private sector, such "opt out" measures would deprive merchants, depository institutions, and issuers of debit and credit cards of any real benefit of RFID.[132] The "access control protocol" measure would essentially turn RFID-tagged cards into ordinary magnetic stripe cards.[133] The "on/off switch" measure and the "radio-reflective shield" measure would prevent depository institutions from using RFID to provide more personalized customer service, since RFID readers cannot read RFID tags that are turned off or encased in radio-reflective shields.[134]

Another example of restrictive legislation is an act introduced in Massachusetts in 2005.[135] This act limits the data that can be stored on RFID tags to information necessary for inventory, product return, recall, or warranty purposes.[136] This act applies to all commercial entities.[137] The act also requires that RFID tags that are not essential to the tagged item's operation be attached in a manner that allows the customer to remove the tag without damaging the item.[138] While the bill's sponsors claim that "[i]n no way does this legislation impinge on the development of the new technology,"[139] the reality is that if this act becomes law, financial institutions would only be able to use RFID for inventory purposes and not to provide more personalized customer service or to implement RFID payment systems.[140]

Although much of the current restrictive legislation was not drafted with financial institutions in mind,[141] the legislation will still

---

132. *See* Garry Boulard, *RFID: Promise or Peril?*, STATE LEGISLATURES MAG., Dec. 2005, at 22 ("[T]he imposition of state regulations on the industry may make obsolete the very service that RFID is designed to provide.").

133. *See* Ala. S. 310 § 4(a)(4).

134. *See supra* text accompanying notes 87, 93.

135. *See* H.R. 1447, 184th Gen. Ct., Reg. Sess. (Mass. 2005).

136. *Id.* § 3.

137. *Id.*

138. *Id.*

139. Sen. Jarrett T. Barrios & Rep. Thomas Kennedy, Regulating Radio Frequency Identification Systems - Fact Sheet, http://www.ncsl.org/standcomm/sctech/MA-RDIFact.htm (last visited Feb. 3, 2007).

140. *See* Mass. H.R. 1447 § 3.

141. *Cf.*, Barrios & Kennedy, *supra* note 139 ("RFID technology was designed to track products while in transit, to ensure against theft, etc. Once a product has been

impact financial institutions.[142] The more restrictions that are placed on the use of RFID, the less appealing the technology becomes to businesses in general.[143] If only a few businesses use RFID technology, then only these few businesses will be equipped to accept RFID payments.[144] Customer interest in RFID payment systems will therefore be low, and it will not be worthwhile for issuers of debit and credit cards to utilize the technology for such purposes.[145] Thus, restrictive legislation will negatively affect use of RFID by issuers of debit and credit cards.[146]

B. Extreme Privacy Legislation

Some states have considered legislation that attempts to regulate unlikely uses of RFID, such as forcible implantation into humans and "Big Brother" tracking of individuals.[147] Such extreme privacy legislation can be found in a recently enacted Wisconsin law that prohibits any person from requiring another individual to have a microchip implanted in his body.[148] Violators may be fined as much as $10,000 each day until the chip is removed.[149] Although the law applies to *any* microchip, it was spurred specifically by concerns over RFID.[150] The law's sponsor admits that there are no known cases of forcible implantation of an

---

purchased, the RFID tag loses its practical value to the retailer, so removing the tag does not affect the retailer or the usefulness of the RFID system.").

142. *Cf.* Piazza, *supra* note 3 ("These various legislative efforts raise concerns among proponents of RFID not only because they would create a hodgepodge of rules but also because they are sometimes overly broad or vaguely worded, potentially impeding the market and making compliance difficult and costly.").

143. *See* Douglas B. Farry, *Does California's New Legislation Ignore Advantages of RFID?*, RFID PRODUCT NEWS, http://www.rfidproductnews.com/issues/2006.09/legal.php (last visited Feb. 3, 2007).

144. *See MasterCard to Test RFID Card*, *supra* note 71.

145. *See id.*

146. *See* Piazza, *supra* note 3.

147. *See, e.g.*, S. 349, 126th Gen. Assem., Reg. Sess. (Ohio 2006); Assem. 290, 97th Leg., Reg. Sess. (Wis. 2006) (enacted); H.R. 7432, 2005-2006 Leg., Jan. Sess. (R.I. 2006) (vetoed June 23, 2006); H.R. 5929, 2005-2006 Leg., Jan. Sess. (R.I. 2005) (vetoed July 15, 2005).

148. Wis. Assem. 290.

149. *Id.*

150. Marc Songini, *Wisconsin Law Bars Forced RFID Implants*, COMPUTERWORLD, June 12, 2006, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=111542.

RFID tag but believes that proactive legislation is crucial.[151] Similarly, in 2006, the Ohio and Missouri legislatures both introduced acts that would prohibit an employer from requiring employees to have RFID tags implanted in their bodies.[152] The Ohio bill's co-sponsors are concerned that employers might want to use RFID to track the movements of their employees both in and out of the workplace.[153] Likewise, in 2005 and 2006, the Rhode Island legislature passed acts that would prohibit state and municipal agencies from using RFID to track the movement of individuals.[154] Although these acts were ultimately vetoed by the governor, they show the extent to which a state legislature distrusts RFID and fears the technology will lead to a "Big Brother" scenario.[155]

Extreme privacy legislation is the most alarmist and unnecessary of all RFID legislation.[156] It assumes the worst possible uses of RFID and then attempts to preemptively regulate them.[157] Although extreme privacy legislation poses the least risk

---

151. *Id.*

152. Ohio S. 349; S. 858, 93rd Gen. Assem., 2nd Reg. Sess. (Mo. 2006). In contrast to the Wisconsin bill, the Ohio bill only imposes a fine of $150 per violation. Ohio S. 349. In contrast to the Wisconsin bill, the Missouri bill only makes the violator guilty of a Class A misdemeanor. Mo. S. 858. A Class A misdemeanor would subject the violator to a fine of no more than $1,000, up to one year imprisonment, or both. Mo. Rev. Stat. § 558.011 (2006); Mo. Rev. Stat. § 560.016 (2006).

153. *RFID News Roundup*, RFID J., July 28, 2006, http://www.rfidjournal.com/article/articleview/2525/1/1/.

154. H.R. 7432, 2005-2006 Leg., Jan. Sess. (R.I. 2006) (vetoed June 23, 2006); H.R. 5929, 2005-2006 Leg., Jan. Sess. (R.I. 2005) (vetoed July 15, 2005).

155. *See* Press Release, The State of R.I. Gen. Assembly, Senate OKs Bill Restricting Use of Radio Tracking Devices (May 23, 2006), *available at* http://www.rilin.state.ri.us/News/pr1.asp?prid=3280. One of the co-sponsors of the Rhode Island bill admitted that there were no known cases of RFID being used to track the movement of individuals but believed that preemptive legislation was necessary to ensure that this does not happen. *Id.* The legislator reasoned that "the terrorist attacks of [September 11, 2001] did make ours a different world in which to live and we now walk a finer line between civil liberties and security. Tagging people with radio tracking devices goes way, way over that line." *Id.*

156. *Cf.* Cline, *supra* note 59 ("The privacy scare surrounding [RFID] is greatly overblown. No company or government agency will be secretly scanning [you or] your house to find out what products you've purchased, because there's no feasible way to do so.").

157. *See, e.g.*, *RFID News Roundup*, *supra* note 153 ("[E]mployers [might] requir[e] employees to have RFID tags embedded into their bodies . . . [and then] use the tags to invade employee's privacy, by tracking their movements within or outside the workplace."); Barrios & Kennedy, *supra* note 139 ("[T]he desire to track

to financial institutions because it does not affect the ways in which financial institutions would want to use the technology, it nevertheless stigmatizes RFID by promoting a sinister characterization of the technology.[158]

C. *Disclosure*

Some state legislation requires those using RFID to disclose to customers that the technology is being used by either placing conspicuous signs at the location of each RFID reader, informing the customer in writing of the location of all readers to be used by the issuing authority, or maintaining and regularly updating a website listing the location of all RFID readers.[159] Disclosure legislation may also require that any product containing an RFID tag bear a symbol or label that notifies the customer that the product contains an RFID tag.[160] A New Hampshire bill goes one step further by stipulating that any product containing an RFID tag must bear a "universally accepted symbol" that indicates the presence of an RFID tag.[161] Currently, however, there is no such symbol.[162] For financial institutions and other businesses to

---

consumers and their purchases often overrides any consideration of maintaining strong customer relations . . . [and l]eft unregulated, [RFID] could lead to near-constant surveillance of consumers without their knowledge.").

158. *See* Songini, *supra* note 150.

159. *See, e.g.*, S. 768, 2005-2006 Leg., Reg. Sess. (Cal. 2005) (vetoed Sept. 30, 2006) (requiring issuing entities to place conspicuous signs at the location of each RFID reader, inform customers in writing of the location of all RFID readers, or maintain a website listing the location of all RFID readers); S. 310, 2006 Leg., Reg. Sess. (Ala. 2006) (requiring issuing entities to either inform customers in writing of the location of all RFID readers or place conspicuous signs at the location of each RFID reader as well as provide a general description of the location of all RFID readers); H.R. 1447, 184th Gen. Ct., Reg. Sess. (Mass. 2005) (requiring issuing entities to place conspicuous signs at the location of each RFID reader).

160. *See, e.g.*, S. 638, 93rd Gen. Assem., 2d Reg. Sess. (Mo. 2006); Mass. H.R. 1447; H.R. 203, 159th Gen. Ct., Reg. Sess. (N.H. 2005).

161. N.H. H.R. 203 (defining "universally accepted symbol" as "a graphical system designed to provide a standard way to show the presence of an RFID transponder, its frequency, and data structure"). This bill makes noncompliance a misdemeanor. *Id.*

162. Mary Catherine O'Connor, *N.H. Reps Approve "Tracking Device" Bill*, RFID J., Jan. 19, 2006, http://www.rfidjournal.com/article/articleview/2093; *see also Could RFID Become Illegal?*, RFID NEWS ONLINE, http://www.rfidnewsonline.com/html/s02_article/article_view.asp?id=127&nav_cat_id=-1&nav_top_id=-1&dsa=0 (last visited Feb. 3, 2007) ("While the [Electronic Product Code (EPC)] Global seal is widely accepted, it can be applied only to EPC-compliant tags and labels. The

comply, they would first need to develop or adopt such a symbol.[163] The New Hampshire bill is therefore an example of legislation that was drafted without a full understanding of its consequences.[164]

Disclosure legislation is more reasonable than restrictive legislation because disclosure legislation does not limit the ways in which RFID can be used and the only burdens that would be imposed on financial institutions are the burdens associated with creating signs and labels or maintaining a website.[165] Furthermore, disclosure legislation is more reasonable than extreme privacy legislation because it does not contribute to an unnecessary stigma regarding RFID, nor is it based on alarmist fears.[166] Disclosure legislation merely alerts consumers when RFID is being used, giving consumers the opportunity to opt out or take whatever measures they deem necessary to protect themselves from any perceived privacy or security threats.[167] Although disclosure legislation is reasonable, it is nevertheless unnecessary because the self-regulatory models proposed by the RFID industry all mandate disclosure of the presence of RFID.[168] Furthermore, it is in a business's best interests to disclose the presence of RFID to customers since failure to do so could result in a loss of customers.[169] Thus, since the RFID industry already recognizes a need for disclosure of RFID, disclosure legislation is unnecessary.[170]

[Association for Automatic Identification and Mobility (AIM)] RFID emblem can be applied to any type of RFID device, but it is not yet universally accepted. AIM has applied to various groups within the International Standards Organization (ISO) to have the emblem included.").

163. *See* O'Connor, *supra* note 162.

164. *Cf. id.* ("This legislation puts the cart before the horse.").

165. *See, e.g.*, Cal. S. 768 § 3; Mo. S. 638; Mass. H.R. 1447.

166. *See* RFID Journal, What is RFID Journal's Position on RFID and Privacy?, http://www.rfidjournal.com/faq/28/129.

167. *See* McIver, *supra* note 59.

168. *See* STAFF OF THE FED. TRADE COMM'N, *supra* note 104.

169. What is RFID Journal's Position on RFID and Privacy?, *supra* note 166.

170. *See* STAFF OF THE FED. TRADE COMM'N, *supra* note 104.

D. *Analysis of RFID Legislation*

Much of the proposed and enacted RFID legislation indicates that legislators believe RFID technology to be "a risky technology requiring specific regulations to prevent identity theft" and protect privacy.[171] Since there have been no incidents of identity theft, forcible implantation, or "Big Brother" tracking involving RFID,[172] these bills simply reflect a "[s]hoot first, ask questions later" viewpoint.[173] If a legislature does not understand RFID, attempts to regulate it are futile.[174] Furthermore, there is a danger that proposed legislation will discourage the use and advancement of the technology.[175] If legislation is too restrictive, it is possible that the pace at which the technology advances in the United States could slow, giving other countries a competitive edge in technological innovation.[176] There is also a danger that state legislation could conflict or vary so greatly among different states that financial institutions operating in multiple states would have trouble complying with the differing state laws.[177]

The effect of some of these bills could be that financial institutions and other businesses may decide that it is not worth the potential costs to employ RFID.[178] If an insufficient number of

---

171. Farry, *supra* note 143.

172. Songini, *supra* note 150; Mark Willoughby, *Opinion: RFID Security Worries Need a Reality Check*, COMPUTERWORLD, May 1, 2006, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=110943&pageNumber=1.

173. Farry, *supra* note 143.

174. *See* Evans, *supra* note 4; *see also* Piazza, *supra* note 3 ("When you have a new technology, a lot of times you have to wait and see where you have demonstrated problems before you can meaningfully regulate them . . . .").

175. *See* Piazza, *supra* note 3; Evans, *supra* note 4; *see also* Letter from Arnold Schwarzenegger to Members of the California State Senate, *supra* note 111.

176. J. Bonasia, *RFID Privacy Concerns Spark a Closer Look by a U.S. Senate Panel*, INVESTOR'S BUS. DAILY, July 18, 2006, at A04 ("U.S. companies have the lead in RFID, but Europe is catching up . . . ."); Evans, *supra* note 4; *see also* Kallender, *supra* note 32 ("Japan's RFID industry is estimated to have been worth nearly $35 million in 2003 and will grow to be worth $221 million by 2010.").

177. *See* Elizabeth Wasserman, *A Prescription for Pharmaceuticals*, RFID J., http://www.rfidjournal.com/article/articleprint/1739/-1/1 (last visited Feb. 3, 2007) ("[D]istributors are concerned that 50 different states might develop 50 different rules that would end up being a compliance nightmare for the industry . . . .").

178. *See* Boulard, *supra* note 132 ("[I]f you begin to regulate [RFID] excessively, it becomes more inefficient, which just destroys the purpose for it in the first place."); *supra* note 142.

businesses adopt RFID to make RFID payment systems feasible, then even the debit and credit card issuers that decide to employ RFID will not fully realize the technology's benefits.[179] Thus, much of the enacted and proposed RFID legislation could deprive issuers of debit and credit cards of some or all of the benefits of RFID.[180] Although disclosure legislation would not have such a negative effect, such legislation is unnecessary since the RFID industry can and will impose a disclosure requirement through self-regulation.[181]

VI. EFFECTIVE EDUCATION MAY RESOLVE WIDESPREAD SECURITY AND PRIVACY FEARS AND LEAD TO MORE EFFECTIVE LEGISLATIVE EFFORTS

Financial institutions can allay privacy fears about RFID by educating their customers, lawmakers, and the general public about the risks of using this technology and their efforts to mitigate these risks through self-regulation.[182] Although education of all lawmakers is important, financial institutions should focus their efforts on state lawmakers since the federal government has already indicated a resistance to federal legislation.[183] Financial institutions may also help put any security and privacy concerns into perspective by comparing RFID to existing technology.[184]

A. Security Concerns

The risk of identity theft and fraud imposed by RFID is arguably no greater than the risk of identity theft and fraud imposed by debit or credit cards.[185] If an RFID tag is stolen, the thief could use the RFID tag to make purchases from the

179. *See MasterCard to Test RFID Card*, *supra* note 71.

180. *See* Boulard, *supra* note 132; Piazza, *supra* note 3.

181. *See* STAFF OF THE FED. TRADE COMM'N, *supra* note 104.

182. *See* Evans, *supra* note 4.

183. *See* STAFF OF THE FED. TRADE COMM'N, *supra* note 104, at 23; Hildner, *supra* note 104, at 151-52.

184. *See* Evans, *supra* note 4 ("Identity technologies face many of the same privacy and security concerns that the World Wide Web and wireless technologies faced early on - and still face today.").

185. *See* Hohman, *supra* note 43.

consumer's account, just like a stolen debit or credit card.[186] One possible security difference between RFID and debit or credit cards is that, presumably, consumers would know when their debit or credit card was stolen and could report it right away, whereas if the data contained on an RFID tag was stolen remotely, the consumer would not know to take action until after there had already been fraudulent activity on the account.[187] Theft of a consumer's debit and credit account information can still occur, however, even without theft of the actual card.[188] A thief can obtain a consumer's debit or credit account information by going through garbage or through an internet scam such as phishing[189] or pharming.[190] This means consumers bear the burden of keeping vigilant watch of their accounts whether or not they use RFID.[191] Nevertheless, if financial institutions want to ease customer

186. *See* Paturi, *supra* note 88.

187. *See* Juels, *supra* note 56 ("[A] thief could potentially duplicate a[n RFID tag] without ever touching it. And he or she can do so without leaving any kind of audit trail . . . .").

188. *See infra* notes 189-90 and accompanying text.

189. THE OFFICE OF THE COMPTROLLER OF THE CURRENCY, INTERNET PIRATES ARE TRYING TO STEAL YOUR PERSONAL FINANCIAL INFORMATION, *available at* http://www.occ.treas.gov/consumer/PhishBrochFINAL-SCREEN.pdf (last visited Feb. 3, 2007) ("In a typical [phishing] case, you'll receive an e-mail that appears to come from a reputable company that you recognize and do business with, such as your financial institution. . . . The e-mail will probably warn you of a serious problem that requires your immediate attention. . . . The e-mail will then encourage you to click on a button to go to the institution's Web site. In a phishing scam, you could be redirected to a phony Web site that may look exactly like the real thing. Sometimes, in fact, it may be the company's actual Web site. In those cases, a pop-up window will quickly appear for the purpose of harvesting your financial information. In either case, you may be asked to update your account information or to provide information for verification purposes: your Social Security number, your account number, your password, or the information you use to verify your identity when speaking to a real financial institution, such as your mother's maiden name or your place of birth.").

190. FED. DEPOSIT INS. CORP., GUIDANCE ON HOW FINANCIAL INSTITUTIONS CAN PROTECT AGAINST PHARMING ATTACKS 1 (2005), *available at* http://www.fdic.gov/news/news/financial/2005/fil6405.pdf ("Pharming refers to the redirection of an individual to an illegitimate [w]eb site through technical means. For example, an [i]nternet banking customer, who routinely logs in to his online banking [w]eb site, may be redirected to an illegitimate [w]eb instead of accessing his or her own bank's [w]eb site.").

191. *Cf.* Hohman, *supra* note 43 (noting that the "worry about whether RFID technology leaves consumers more vulnerable to identity and privacy theft" is unfounded because "[n]othing is being done with RFID that isn't already being done with credit cards today . . . .").

security concerns, they can offer to send their customers daily e-mails listing all transactions posting that day.[192]

Furthermore, like RFID tags, debit and credit cards can be cloned and the actual card does not have to be "stolen" in order to be cloned.[193] A bartender, waiter, or other store employee could carry a scanning device small enough to fit in a pocket or on a belt.[194] The scanning device copies the information from the debit or credit card's magnetic strip, which allows the employee to later copy the information to a counterfeit card.[195] When customers hand their debit or credit card to the employee for payment, the employee could quickly swipe the card through the scanning device.[196] It is possible that customers would not notice this suspicious activity even if it was done in their presence.[197] In this respect, RFID might actually be safer than debit or credit cards because it eliminates the number of times consumers have to hand their cards over to another party.[198] In addition, unlike debit or credit cards, the data contained on an RFID tag is encrypted, making the data useless to the thief if the thief does not know how to "crack" an encryption key.[199] Moreover, today's computers are not capable of "cracking" a 128-bit encryption key, which RFID tags could employ.[200]

Financial institutions should also stress that they would already be liable for financial losses from fraudulent use of a stolen or cloned RFID tag,[201] whether the liability is imposed under

192. *See, e.g.* Bank of America, Privacy & Security, Our Products Are Secure, Online Banking, https://www.bankofamerica.com/privacy/Control.do?body=privacy secur_olb (last visited Feb. 3, 2007).

193. Creditnet, How Do Credit Cards Get Cloned?, http://consumers.creditnet.com/Library/Credit_Card_FAQ/How_do_credit_cards_get_cloned.ccfaq_019.php (last visited Feb. 3, 2007).

194. *See id.*

195. *Id.*

196. *Id.*

197. *Id.*

198. Noe, *supra* note 46.

199. *See* Schwartz, *supra* note 81; How Do Credit Cards Get Cloned?, *supra* note 193.

200. WILLIAMS, *supra* note 80.

201. Hohman, *supra* note 43 ("All the same rules and regulations that apply to credit and debit cards apply to [RFID] cards . . . .").

company policy[202] or under the rules and regulations that currently apply to credit and debit cards, such as Regulation E and the Truth in Lending Act.[203] Thus, financial institutions may overcome security concerns by explaining to their customers, lawmakers, and the general public that the risk of and liability for identity theft and fraud imposed by RFID is no greater than, and is possibly even less than, the risk of and liability for identity theft and fraud imposed by debit or credit cards.[204]

B. Privacy Concerns

The privacy concerns raised by opponents to RFID are very similar to the privacy concerns that exist with respect to existing technologies.[205] Wireless phones come equipped with Global Positioning System (GPS) technology and can thus be used to track the movement of customers,[206] supermarkets use loyalty cards to track the purchases of customers and to issue targeted advertising,[207] and credit card companies track the buying patterns of customers.[208] Furthermore, since the rules and regulations that apply to credit and debit cards will already apply to RFID, consumer privacy will be protected to the extent that it is protected under existing laws,[209] such as the Gramm-Leach-Bliley

---

202. *See* Schwartz, *supra* note 81 (noting that Visa, MasterCard, and American Express have all stated that RFID cardholders are not liable for fraud resulting from stolen or cloned information).

203. 12 C.F.R. §§ 205.1-205.18 (2005); Truth in Lending Act, Pub. L. 90-321, §§ 101-145, 82 Stat. 146, 146-59 (1968) (codified as amended in scattered sections of 15 U.S.C.). For debit cards, Regulation E provides that if the consumer notifies the financial institution of an unauthorized debit within two business days after learning of the unauthorized debit, the consumer's liability is limited to fifty dollars. 12 C.F.R. § 205.6(b)(1) (2005). If the consumer fails to notify the financial institution within this time period, the consumer's potential liability increases to $500. *Id.* § 205.6(b)(2). For credit cards, the Truth in Lending Act provides that the consumer's liability for unauthorized use is limited to fifty dollars. Truth in Lending Act § 133(a) (codified as amended at 15 U.S.C. § 1643(a) (2000)).

204. *See* Noe, *supra* note 46; Hohman, *supra* note 43; *MasterCard to Test RFID Card*, *supra* note 71.

205. *See* Hohman, *supra* note 43.

206. *See id.*

207. Piazza, *supra* note 3; Hohman, *supra* note 43.

208. *See* Hohman, *supra* note 43.

209. *See id.*

Act,[210] the Fair Credit Reporting Act,[211] and the Electronic Communications Privacy Act.[212] This means that a financial institution would already have a legal obligation to ensure that customer information is kept confidential and is adequately protected from unauthorized access.[213] Also, if a financial institution plans on sharing a customer's information with companies with which it is not affiliated, the customer would be entitled to receive a privacy notice from the financial institution.[214] Customers would be able to opt out of having their information shared with certain third parties not affiliated with the financial institution[215] and financial institutions would be prohibited from disclosing their customers' account numbers to non-affiliated companies for telemarketing, direct mail marketing, or other marketing through e-mail, even if the customers had not opted out of sharing the information for marketing purposes.[216] Furthermore, neither the financial institution nor a third party could intentionally read the customer's RFID tag without the customer's authorization.[217] Thus, consumer privacy protections

210. 15 U.S.C. §§ 6801-6827 (2000). The Gramm-Leach-Bliley Act applies to all consumer personal financial information held by financial institutions. FED. TRADE COMM'N, IN BRIEF: THE FINANCIAL PRIVACY REQUIREMENTS OF THE GRAMM-LEACH-BLILEY ACT, http://www.ftc.gov/bcp/conline/pubs/buspubs/glbshort.pdf (last visited Feb. 3, 2007).

211. 15 U.S.C. §§ 1681-1681x (2000).

212. Electronic Communications Privacy Act, Pub. L. 99-508, 100 Stat. 1848 (1986) (codified in scattered sections of 18 U.S.C.). Since RFID will likely be deemed to be electronic communication, the Electronic Communications Privacy Act (ECPA) will also apply. *See* Reuven R. Levary et al., *RFID, Electronic Eavesdropping and the Law*, RFID J., Feb. 14, 2005, http://www.rfidjournal.com/article/articleview/1401/1/128/.

213. 15 U.S.C. § 6801 (2000).

214. *Id.* § 6803. Consumers with a *continuing* relationship with the financial institution are entitled to receive a yearly privacy notice from the financial institution for the duration of the relationship, regardless of whether the financial institution shares information with companies with which it is not affiliated. FED. TRADE COMM'N, *supra* note 210.

215. 15 U.S.C. § 6802(b)(1)(B) (2000); *id.* § 1681s-3(a)(2) (2000).

216. 15 U.S.C. § 6802(d) (2000).

217. 18 U.S.C. § 2511 (2000). The ECPA prohibits any person from intentionally intercepting or endeavoring to intercept electronic communications by using an electronic, mechanical, or other device unless the conduct is specifically authorized or expressly not covered. *Id.*

are the same whether the financial institution uses RFID or magnetic stripe cards.[218]

VII. CONCLUSION

For customers, the potential benefits of RFID are the convenience of drastically reduced transaction times and more personalized customer service.[219] For financial institutions, using RFID may allow for more efficient document-tracking and increased data security and also enable them to more effectively market their products and provide faster, more personalized service to customers.[220] As RFID rapidly continues to advance and more entities consider utilizing this technology, several state legislators have responded by introducing or passing unnecessary legislation concerning RFID, much of which could have the effect of inhibiting use and expansion of the technology.[221]

If legislation hinders the advancement of RFID, the costs of implementing a secure RFID system that protects consumer privacy will continue to outweigh the benefits.[222] Thus, businesses and financial institutions will forgo incorporating RFID, and the benefits of this technology will never be fully recognized.[223] In order to counteract this prohibitive effect, financial institutions need to be proactive in educating their customers, lawmakers and the general public to ensure that unnecessary RFID legislation is not passed.[224]

KRISTINA M. WILLINGHAM

218. *See id.*; Levary et al., *supra* note 212.

219. *See supra* text accompanying notes 21-27, 37-46.

220. *See supra* notes 20-46 and accompanying text.

221. *See supra* notes 118-70 and accompanying text.

222. *See supra* notes 178-80 and accompanying text.

223. *See supra* notes 178-80 and accompanying text.

224. *See supra* notes 182-218 and accompanying text; *see also* Mark R. Madler, *Bills Threaten Burgeoning RFID Business*, SAN FERNANDO VALLEY BUS. J., May 22, 2006 (noting that education of the public, lawmakers, and the media should be one of the goals of the industry to help counter misinformation about RFID).