Marquette Intellectual Property Law Review

Volume 11 | Issue 1 Article 6

Gone in a Blink: The Overlooked Privacy Problems Caused by Contactless Payment Systems

Shane L. Smith

WINNER OF THE COMPUTER LAW ASSOCIATION 2006 INFORMATION TECHNOLOGY LAW WRITING COMPETITION

Gone in a Blink: The Overlooked Privacy Problems Caused by Contactless Payment Systems

INTRODUCTION

"The free man is the private man . . . ."[1]

More than a century ago, two scholars[2] sparked a debate that will probably never end: whether individuals possess a right to privacy and, if so, the nature and extent to which the law should protect privacy rights.[3] Since that first argument, the debate has ranged—and escalated—from whether such a "right 'to be let alone'"[4] truly exists,[5] to when and under what circumstances a person's privacy rights are violated.[6] The debate seems to crescendo with the introduction of new technologies.[7] The push for global adoption of electronic product code (EPC) tags as replacements for universal product code (UPC) bar codes sparked one of the more recent debates.[8] The chief concern of privacy

1. Clinton Rossiter, *The Pattern of Liberty*, *in* ASPECTS OF LIBERTY: ESSAYS PRESENTED TO ROBERT E. CUSHMAN 15, 17 (Milton R. Konvitz & Clinton Rossiter eds., 1958).

2. I refer, of course, to Samuel D. Warren and Louis D. Brandeis and their seminal *Harvard Law Review* article on individuals' privacy rights. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

3. *Id.* at 197.

4. *Id.* at 195 (quoting THOMAS M. COOLEY, A TREATISE ON THE LAW OF TORTS OR THE WRONGS WHICH ARISE INDEPENDENT OF CONTRACT 29 (Alexis C. Angell ed., 2d ed., Chicago, Callaghan & Co. 1888)).

5. *Compare id.* at 214 (asserting that rules for limiting and remedying the right to privacy may be found in "legal analogies already developed in the [common] law of slander and libel and in the [common] law of literary and artistic property"), *with* Katz v. United States, 389 U.S. 347, 374 (1967) (Black, J., dissenting) ("No general right [to privacy] is created by the [Fourth] Amendment . . . ."), *and* Griswold v. Connecticut, 381 U.S. 479, 484–86 (1965) (asserting there is a "right of privacy older than the Bill of Rights," and even though not enumerated, "specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance" and "create zones of privacy").

6. *See, e.g.*, United States v. Place, 462 U.S. 696, 707 (1983) (stating, in dicta, that a dog sniff of a person's luggage for illicit drugs does "not constitute a 'search' within the meaning of the Fourth Amendment," and, by extension, does not constitute a privacy violation because "this investigative technique is much less intrusive than a typical search"). *But see* Kyllo v. United States, 533 U.S. 27, 40 (2001) ("Where . . . the Government uses a device that is not in general public use, to explore details of a private home that would previously have been unknowable without physical intrusion, the surveillance is a Fourth Amendment 'search' and is [a] presumptively unreasonable [violation of privacy] without a warrant.").

7. *See, e.g.*, ALAN F. WESTIN, PRIVACY AND FREEDOM 304 (1967) (recalling that when the U.S. National Office of Vital Statistics proposed replacing social security numbers with national birth certificate numbers, the "idea was denounced . . . as a potentially regimenting 'police state' measure, and angry cartoons raised the 'Big Brother' argument," causing enough opposition to kill the idea).

8. EPC tags are radio frequency identification (RFID) enabled microchips with enough memory capacity to store an electronic product code (EPC). *See RFID Technology: What*

advocates appears to be that EPC tags would permit individuals to be surreptitiously profiled and tracked.[9] Just like earlier debates involving technology and privacy, the war of words over the planned implementation of EPC tags has become quite robust. In addition, the possible use of radio frequency identification (RFID) technology in certain government-issued identification cards—for example, drivers' licenses, student identification cards, and government health and benefit cards—has received considerable attention.[10]

By contrast, an issue that has received little, if any, attention from privacy advocates is the use of RFID technology in contactless payment devices such as MasterCard's PayPass card, Chase Card Service's (Chase) blink card, or ExxonMobil's Speedpass key fob.[11] The

the Future Holds for Commerce, Security, and the Consumer: Hearing Before the Subcomm. on Commerce, Trade, and Consumer Protection, 108th Cong. 10 (2004) [hereinafter *Hearing*] (prepared statement of Sanjay Sarma, Assoc. Professor, Mass. Inst. Tech.). EPCs are identification numbers of sufficient length to allow for trillions of unique numbers—enough to assign a unique EPC to all items produced worldwide. *Id.* at 10–13; *see also* Privacy Rights Clearinghouse (PRC), RFID Position Statement of Consumer Privacy and Civil Liberties Organizations (Nov. 20, 2003), http://www.privacyrights.org/ar/RFIDposition.htm [hereinafter RFID Position Statement].

9. *See, e.g.*, KLAUS FINKENZELLER, RFID HANDBOOK: FUNDAMENTALS AND APPLICATIONS IN CONTACTLESS SMART CARDS AND IDENTIFICATION 1 (Rachel Waddington trans., 2d ed., John Wiley & Sons Ltd. 2003) (1999).

10. *See, e.g.*, Electronic Frontier Foundation (EFF), Fact Sheet: Senate Bill 768 (Simitian), http://www.eff.org/Privacy/Surveillance/RFID/sb682_fact_sheet.php (last visited Dec. 22, 2006) (rallying support for California's proposed Identity Information Protection Act of 2006); *see also Identity Information Protection Act: Hearing on S.B. 682 Before the S. Judiciary Comm.*, 2005–2006 Leg., Reg. Sess. (Ca. 2005), *available at* http://info.sen.ca.gov/pub/05-06/bill/sen/sb_0651-0700/sb_682_cfa_20050518_122757_sen_comm.html; Lee Tien, Senior Staff Att'y, EFF, Prepared Testimony Before the S. Judiciary Comm. in Support of the Identify Information Protection Act (S.B. 682) (Apr. 26, 2005), http://www.eff.org/Privacy/Surveillance/RFID/tien_testimony_sb_682.pdf.

11. Although contactless payment proponents assert that contactless payment devices and RFID are "fundamentally different," contactless payment devices operate on chip-level radio frequency technology just like all other RFID-enabled devices and are only "different" from other RFID-enabled devices in the sense that contactless payment devices have added "smart chip technology." SMART CARD ALLIANCE, THE WHAT, WHO AND WHY OF CONTACTLESS PAYMENTS 2–4, 6 (2006), http://www.smartcardalliance.org/resources/pdf/CP_What_Who_Why_Final.pdf [hereinafter SMART CARD ALLIANCE WHITE PAPER]. In other words, the only difference is that in addition to containing an RFID transponder, contactless payment devices contain a microcontroller capable of executing a cryptographic operation designed to create a unique transaction validation number for every transaction. *See* David Birch, *Contactless Payments and the Security Challenges*, ITADVISER, July/Aug. 2005, http://www.nccmembership.co.uk/pooled/articles/BF_WEBART/view.asp?Q=BF_WEBART_171100. Mark Baard of *Wired News* provides a more frank assessment of the difference:

[T]he Homeland Security Department is very carefully avoiding use of the term

"contactless smart chips"[12] powering these contactless payment devices can be embedded in countless form factors such as mobile phones, wristwatches, or money clips,[13] all for the purpose of replacing customers' traditional credit and debit card plastics with magnetic stripes. Such wearable or pocketable form factors may soon be supplanted by the next generation of contactless payment devices: contactless smart chips implanted subdermally in humans.[14] While the purported technological limitations and security features of the types of RFID-enabled smart chips used in contactless payment devices may appear to mitigate *security* concerns,[15] the *privacy* concerns caused by contactless payment devices in any form factor appear to have been overlooked. Such a discussion should not be delayed until, for example, contactless payment systems experience "function creep" to be used for other purposes. What if, for example, contactless payment devices become so widely distributed that the government realizes it can profile

> "RFID." The department, along with Philips, is also backing a trade group that is branding ID documents with RFID tags as "contactless smartcards."
>
> "We'd prefer," said Joseph Broghamer, Homeland Security's director of authentication technologies, "that the terms 'RFID,' or even 'RF,' not be used at all . . . [when referring to contactless devices]. Let's get 'RF' out of it altogether."

Mark Baard, *RFID Cards Get Spin Treatment*, WIRED NEWS, Mar. 29, 2005, http://www.wired.com/news/privacy/0,1848,67025,00.html.

12. A contactless smart chip is "[a]n integrated circuit (IC) that includes a secure microcontroller or equivalent intelligence and internal memory, and communicates with a reader through a radio frequency (RF) interface." Smart Card Alliance, Contactless Payments Glossary 1, http://www.smartcardalliance.org/resources/pdf/contactless_pmt_glossary.pdf (last visited Dec. 22, 2006) [hereinafter Glossary].

13. *See* Evan Schuman, *MasterCard Pursues No-Touch Retail*, EWEEK, Oct. 9, 2005, http://www.eweek.com/article2/0,1759,1868307,00.asp?kc=EWRSS03119TX1K0000594 [hereinafter Schuman, *No-Touch Retail*]; *see also* David Enrich, *Money Clips, Jewelry May Act as Substitutes for Credit Cards*, WALL ST. J., Sept. 6, 2005, at D3.

14. The VeriChip, a subdermally-implantable active contactless smart chip introduced by Applied Digital Solutions, Inc. (Applied Digital), features a financial services application enabling it to be used for contactless payments. Applied Digital announced its VeriPay contactless payment system based on the VeriChip in November 2003. *See* Press Release, Applied Digital Solutions, Applied Digital Solutions' CEO Announces "VeriPay" Secure, Subdermal Solution for Payment and Credit Transactions at ID World 2003 in Paris (Nov. 21, 2003), *available at* http://web.archive.org/web/20031207111617/http://www.adsx.com/news/2003/112103.html. "VeriPay is intended to be a secure, subdermal RFID . . . payment technology for cash and credit transactions." *Id.* VeriPay is being tested at the Baja Beach Club in Barcelona, Spain, where patrons injected with a VeriChip pay for drinks and other such things with the wave of a hand. *See* Press Release, VeriChip, Applications Continue to Grow for Applied Digital Solutions' VeriPay Baja Beach Club in Barcelona, Spain Employs RFID Technology for Cashless Payment System (Apr. 5, 2004), *available at* http://www.verichipcorp.com/news/1081144800.

15. *See infra* notes 34–39, 68–69 and accompanying text.

and track individuals through their contactless payment devices rather than battle public opposition to RFID-enabled identification cards under the Real ID Act?[16] What if the public so opposes EPC tags as UPC bar code replacements in consumer products that businesses have to scrap the idea, but businesses then realize they can profile and track individuals for marketing purposes just the same by interrogating contactless payment devices? Ultimately, it does not matter whether RFID-enabled smart chips are used in identification cards, whether EPC tags are ever adopted as UPC bar code replacements in consumer products, or whether banks and merchants ever issue subdermal contactless payment devices; contactless payment devices already provide a reliable infrastructure for profiling and tracking individuals.

EPC-tagged consumer products are likely years away from being ubiquitous and no RFID-enabled identification cards have been issued to civilians in the United States. In contrast, more than eight million Americans already carry and use contactless payment devices.[17] Although EPC-tagged consumer products and RFID-enabled, government-issued identification cards may be years away from providing the beginnings of a surveillance infrastructure, contactless payment devices are quietly and quickly creating a surveillance infrastructure today. Contactless payment systems provide a more reliable infrastructure for tracking and profiling individuals than would EPC-tagged consumer products because many product purchases are not for the purchaser's own consumption. Individuals often purchase consumer products as gifts for others, thus any attempt to profile or track the purchaser using EPC tags in those products would be an exercise in futility. Similarly, individuals frequently discard broken or worn-out products and dispose of unwanted products—a reality that would limit opportunities to profile or track the purchaser and, at a minimum, render the collected data questionable since no one would know if or when the purchaser discarded or disposed of any particular product. In contrast, a contactless payment device issued to a particular individual is highly likely to be carried by that individual nearly everywhere he or she goes, never given as a gift or otherwise permanently transferred to another person, and never intentionally discarded. While contactless payment systems may create the optimal

16. Real ID Act of 2005, Pub. L. No. 109-13, div. B, 119 Stat. 231, 302 (2005) (codified as amended in scattered sections of 8 U.S.C.). Title II of the Act deals with improved security for drivers' licenses and personal identification cards. *Id.*

17. *See infra* notes 52, 70.

surveillance infrastructure, privacy advocates and lawmakers appear not to have noticed.[18]

Part I briefly describes what RFID is and how it works and explains why contactless payment systems are likely to provide the best solution to accomplish the goals of banks and merchants to achieve '"convenience, speed and ease of use to consumers'" and increase profitability as a result of '"faster transaction times and increased spending per transaction.'"[19] Part II briefly describes privacy advocates' focus on the privacy problems caused by every RFID application *except* contactless payment systems, discusses the privacy problems caused by contactless payment systems, and reveals the resulting hole in the privacy debate. Part III argues that the proposals for self-regulation or legislation that have been developed by privacy advocates and RFID proponents fail to address the privacy concerns implicated by contactless payment systems. The Article concludes with a proposed legislative response sufficient to address privacy concerns without stifling technological development.

I. BANKS, MERCHANTS, AND CONSUMERS: PRIMED FOR CONTACTLESS PAYMENT TECHNOLOGY

A. RFID in a Contactless Payment System Nutshell

In the context of a contactless payment system, RFID is the system for transmitting all of the details of a payment transaction between a merchant and the issuer of a contactless payment device. Stripped of technical details, a typical contactless payment transaction flows according to the following progressive steps. At the checkout register, the customer briefly holds his or her contactless payment device near the merchant's point-of-sale terminal (POS terminal), which houses an RFID reader that "connects to, provides power to and communicates with" the contactless payment device.[20] The reader interrogates the contactless payment device, receives the device's EPC and a

18. *See* discussion *infra* Part III.A.

19. Press Release, Market Wire, New Smart Card Alliance Council Created to Inform Issuers, Merchants and Consumers About Benefits of Contactless Payments (Aug. 30, 2005) (quoting Randy Vanderhoof, Executive Dir., Smart Card Alliance), *available at* http://press.arrivenet.com/technology/article.php/687018.html.

20. Glossary, *supra* note 12, at 2. RFID readers only need to provide power to contactless payment devices employing passive RFID, as passive RFID devices do not have their own power source. *See infra* notes 27–28 and accompanying text.

cryptogram[21] for that transaction, and transmits the transaction details to the merchant's acquiring bank.[22] The acquiring bank, in turn, transmits the transaction data to the issuing bank.[23] The issuing bank uses the contactless payment device's EPC to identify the correct customer's account and uses the cryptogram to confirm the device's validity.[24] The issuing bank then returns an authorization, decline, or other appropriate response, and the customer goes on his or her way.

A contactless payment system's operation depends primarily on two RFID components: an RFID reader housed in a POS terminal, as described above; and a "contactless smart chip"—a "secure microcontroller or equivalent intelligence, internal memory, and a small antenna," which "communicates with a reader through a contactless

21. The cryptogram is a one-time code calculated inside the contactless payment device that serves as a unique validator for the instant transaction. The cryptogram is comprised of the device's EPC *plus* a transaction counter encrypted by a security key inserted in the contactless payment device during manufacturing. This security key is derived from the device's EPC and the issuing bank's master key. Once inserted into the contactless payment device, the security key is never divulged. According to one source:

> This kind of solution provides: Privacy, because the [contactless payment device's unique] ID is meaningless to anyone other than the issuing bank which can map that ID to an actual account or card number; [and] Security, because knowing the . . . [contactless payment device's] ID is insufficient to create a cloned . . . [contactless payment device]. Also, a cloned . . . [contactless payment device] would not generate a correct cryptogram because it would not have the right security key[,] and if the transaction is replayed[,] the transaction counter will be wrong.

Birch, *supra* note 11. Birch's assertion that contactless payment devices provide failsafe privacy does not acknowledge the problem of identity theft. Even if none of an individual's nonpublic personal information is ever stored on a contactless payment device, the device's unique EPC is very meaningful to an identity thief who has other means to gain nonpublic personal information about his victim. *See infra* notes 65–95 and accompanying text. Moreover, the victim's credit, debit, or other account number and other personal information may not be encrypted. *See infra* note 74 and accompanying text. Identity theft is a massive problem: the Federal Trade Commission (FTC) received reports of 255,565 cases of identity theft in 2005. *See* FED. TRADE COMM'N, CONSUMER FRAUD AND IDENTITY THEFT REPORT DATA 4 (2006), *available at* http://www.consumer.gov/sentinel/pubs/Top10Fraud 2005.pdf.

22. Birch, *supra* note 11.

23. *Id.*

24. *Id.*

radio frequency (RF) interface."[25] These microchips used in contactless payment devices feature either "passive" or "active" RFID.[26]

Contactless payment devices that employ passive RFID smart chips have no onboard battery, a feature that makes their life span virtually unlimited and their design compact.[27] Because they have no internal power source, they do not continuously transmit data, but rather "wake up" to respond to a radio signal from any RFID reader.[28] Generally, passive smart chips are read-only, meaning the data they contain cannot be altered or written over.[29] Privacy advocates have focused their attention almost exclusively on the type of passive microchips used in EPC tags to replace UPC bar codes[30] rather than on the passive smart chips used in most contactless payment devices.[31]

The privacy concerns over the passive microchips in EPC tags seem to stem from four factors. First, the tiny size of the passive microchips used in EPC tags could make them difficult, if not impossible, to locate once embedded in an object.[32] Currently, "the smallest . . . [passive microchips] measure[] 0.15 mm × 0.15 mm, and are thinner than a sheet of paper."[33] In contrast, the passive smart chips used in some contactless payment devices may be as large as a one-inch-long glass or plastic

25. SMART CARD ALLIANCE, CONTACTLESS SMART CHIP TECHNOLOGY: THE BUSINESS BENEFITS 1 (2005), http://www.smartcardalliance.org/resources/pdf/contactless_business_benefits.pdf. Because of their "secure microcontroller or equivalent intelligence," proponents of contactless payment devices have dubbed these microchips as "smart chips." *Id.*

26. *See* RFID 101: About RFID Tags & Transponders for Radio Frequency Identification, http://www.rfid-101.com/rfid-tags.htm (last visited Dec. 22, 2006) [hereinafter RFID 101].

27. *See* Stephen C. Bono et al., Security Analysis of a Cryptographically-Enabled RFID Device, Refereed Paper at 14th USENIX Security Symposium (Aug. 3, 2005), *available at* http://www.usenix.org/events/sec05/tech/bono/bono.pdf.

28. RFID 101, *supra* note 26.

29. Birch, *supra* note 11.

30. *See generally* RFID Position Statement, *supra* note 8.

31. *See* discussion and notes *infra* Parts II, II.A. Not all contactless payment devices employ passive RFID; some use low-frequency, active RFID technology. *See infra* note 100 and accompanying text.

32. *See* Oleg Kobelev, Recent Development, *Big Brother on a Tiny Chip: Ushering in the Age of Global Surveillance Through the Use of Radio Frequency Identification Technology and the Need for Legislative Response*, 6 N.C. J.L. & TECH. 325, 331 (2005).

33. Wikipedia, Radio Frequency Identification, http://en.wikipedia.org/wiki/RFID (last visited Dec. 22, 2006) [hereinafter Wikipedia RFID]; *see also* Yoshiko Hara, *Hitachi Advances Paper-Thin RFID Chip*, EE TIMES, Feb. 2, 2006, http://www.eetimes.com/news/design/showArticle.jhtml?articleID=179100286.

capsule.[34] Second, since passive microchips of all types have no onboard battery, they cannot be turned off[35] and are, thus, susceptible to being accessed and read by unauthorized RFID readers. Third, the frequency on which RFID-enabled microchips operate dictates their read range. The high frequency on which the passive microchips used in EPC tags operate could permit an RFID reader to read an EPC tag's data from distances of up to twenty feet.[36] In contrast, the passive smart chips used in most contactless payment devices operate on a low frequency, which contactless payment system proponents claim limits the read range of contactless payment devices to no more than four inches.[37] Finally, while the passive microchips in EPC tags used as UPC bar code replacements feature no encryption capability, the passive smart chips used in contactless payment devices contain a microcontroller capable of executing a complex cryptographic operation, albeit with varying levels of encryption,[38] to create a unique transaction validation number for every transaction.[39]

Unlike passive RFID microchips, which have no battery and must be interrogated by a reader in order to communicate data, active RFID microchips contain a battery-powered transmitter that is constantly on,[40] enabling them to provide information to an RFID reader on demand or provide information voluntarily.[41] Active microchips are generally larger than passive microchips, with the smallest currently ranging in

34. *See, e.g.*, Bono et al., *supra* note 27, at 2; *see also* RFID/EPC Technology Solutions, 23mm Glass Capsule Transponder DST, http://www.ti.com/rfid/shtml/prod-trans-RI-TRP-BRHP.shtml (last visited Dec. 22, 2006).

35. *See* Kobelev, *supra* note 32, at 331.

36. RFID 101, *supra* note 26. According to the Electronic Privacy Information Center (EPIC), "industry experts say plans for building far more sensitive RFID signal receivers are in the works" so this range is likely to increase significantly within the coming years. EPIC RFID Privacy Page, http://www.epic.org/privacy/rfid/ (last visited Dec. 22, 2006).

37. Glossary, *supra* note 12, at 1. This claim, however, is clearly not true. *See* Liz Pulliam Weston, *New Credit Cards Allow Hands-Free Theft*, MSN MONEY, http://articles.moneycentral.msn.com/Banking/CreditCardSmarts/NewCreditCardsAllowHandsFreeTheft.aspx (last visited Dec. 22, 2006).

38. *See infra* notes 69–71 and accompanying text.

39. *See* Geoff MacGillivray, *Understanding the Different Memory Types Used in Contactless Smart Cards and RFID Tokens*, CONTACTLESS NEWS, Oct. 8, 2005, http://www.contactlessnews.com/library/2005/10/08/understanding-the-different-memory-types-used-in-contactless-smart-cards-and-rfid-tokens/.

40. RFID 101, *supra* note 26.

41. Tom Kevan, *Active RFID Is Redefining Wireless Infrastructure*, FRONTLINE SOLUTIONS, Oct. 2004, *available at* http://www.sensitech.com/pdfs/Active_RFID_Redefines.pdf.

size from a grain of rice[42] to a small coin.[43] Active RFID microchips are also able to contain much more data than passive microchips, "commonly provid[ing] 1 million bits of dynamically searchable data storage,"[44] and are read-writable, meaning the data they contain can be repeatedly written over and changed.[45] Although the contactless payment devices currently being distributed widely in the United States use passive RFID smart chips, it is important to keep in mind that the use of active RFID smart chips in contactless payment devices would enable those devices to do double duty as both contactless payment devices and contactless payment device readers.[46]

B. Why Is Contactless Payment Technology Appealing?

Proponents of contactless payment systems are sold on—or are selling—the idea that contactless payment systems will yield major benefits: faster, more convenient, and more secure payment transactions for consumers; and greater profits for banks and merchants.[47] Banks and merchants tout these speed, convenience, and security virtues in their marketing efforts to push contactless payment devices into customers' hands,[48] but their real motive appears to be

42. *See* VeriChip Corporation, RFID Tags, http://www.verichipcorp.com/content/company/rfidtags (last visited Dec. 22, 2006).

43. *See* Wikipedia RFID, *supra* note 33.

44. Kevan, *supra* note 41, at 2.

45. RFID 101, *supra* note 26.

46. *See infra* note 100.

47. The Smart Card Alliance boasts the membership of hundreds of U.S. and international organizations and institutions. *See* Smart Card Alliance, Current Members, http://www.smartcardalliance.org/about_alliance/current_members.cfm (last visited Dec. 22, 2006) [hereinafter Smart Card Alliance Current Members]. Alliance members share a common mission to "stimulate the understanding, adoption, use and widespread application of smart card technology." Smart Card Alliance, About the Alliance, http://www.smartcardalliance.org/about_alliance/mission.cfm (last visited Dec. 22, 2006). If individual banks and merchants are not already sold on contactless payment system technology on their own, they will be soon; Alliance members include MasterCard International, Visa USA, and American Express. *See* Smart Card Alliance Current Members, *supra*. In the consumer payment transactions world, as MasterCard and Visa go, so goes everyone—this is so because MasterCard and Visa generally require such cooperation from banks and merchants in their card acceptance agreements or otherwise create incentives too great for banks and, especially, merchants to ignore.

48. Claims of faster transaction speeds involve much smoke and mirrors. The only merchants able to shave significant amounts off of transaction processing times are those in the quick-serve restaurant category, specifically those with drive-through lanes. *See, e.g.*, *Contactless Payments in a 'blink*,' RFID NEWS, May 23, 2005, http://www.rfidnews.org/news/2005/05/23/contactless-payments-in-a-blink/ ("The most significant timesavings [sic] can be realized in the drive-thru environment, where transaction time was reduced by as much as 20

greater profits. Carter Frank, chief marketing officer at Chase explained: "[T]hese innovative [contactless] cards . . . . will provide merchants and our cobrand partners with an opportunity to build even stronger customer loyalty programs."[49] According to the Smart Card Alliance, merchants are especially attracted to contactless payment systems because "increased customer loyalty increase[s] revenues."[50]

seconds as compared to cash."). In reality, payment transaction processing speeds are limited by each merchant's means of routing payment authorization transactions to and from the merchant's acquiring bank. In the United States, most merchants' POS terminals dial out on regular telephone lines to transmit transaction details and receive the issuing bank's response. It may be a few seconds faster to wave a contactless payment device near an RFID reader than to swipe a magnetic stripe on a card, but that has always been the fastest portion of any credit or debit card transaction. Until *all* merchants implement faster transaction routing technology, including use of communication systems such as satellite or "always-on" DSL Internet access, payment transaction processing speeds will remain slow. Further, in making these speedy transaction claims, banks and merchants avoid calling attention to the fact that the payment processing step is only a tiny portion of the slow transaction problem. Until EPC tags see widespread use as UPC bar code replacements, customers will still have to wait for UPC bar codes to be manually—and individually—scanned. *See, e.g.*, Evan Schuman, *Who's Afraid of the Big Bad Chase?*, EWEEK, May 26, 2005, http://www.cioinsight.com /print_article2/0,1217,a=152846,00.asp [hereinafter Schuman, *Big Bad Chase*] ("When you cut through the hype, all you have is a card that can shave a few seconds—maybe a fraction of a minute—off of a transaction. . . . [T]he initial contactless card will still likely live in a wallet inside a pocket, which requires time to pull out."). These current realities will not likely dampen consumers' enthusiasm for faster, more convenient payment methods such as contactless payment systems. The "microwave" and later generations have developed an appetite for speed, convenience, and nifty electronic gadgets and will expect banks and merchants to deliver on each of those fronts.

Convenience claims, on the other hand, appear accurate. MasterCard International's research "found that nearly half of the country's consumers carry $20 or less in their wallets and 86 percent of the people surveyed said that they would like to lessen the number of times that they use cash." Christian Meagher, *Contactless Payments Take the Plunge*, ECOMMERCE, Sept. 15, 2004, http://www.insideid.com/ecommerce/article.php/3408481. Ubiquitous acceptance of contactless payment transactions would dispense with the need to carry cash for any payment transaction—from your corner grocery store to your neighbor's garage sale and to every vending machine in between.

Security claims lack merit. *See infra* notes 65–95 and accompanying text, particularly note 74.

49. *Contactless Payments in a 'blink,' supra* note 48. Similarly, MasterCard claims its PayPass contactless payment system will allow banks and merchants to increase market share because the system is "way speedier than *cash*" transactions—not "way speedier" than traditional credit and debit card transactions. The RFID Weblog: MasterCard Contactless Payment System Headed to National Rollout, http://www.rfid-weblog.com/archives/ mastercard_contactless_payment_system_headed_to_national_rollout.html (last visited Dec. 22, 2006) (emphasis added); *see also* Alorie Gilbert, *MasterCard Tests High-Tech Payments*, ZDNET NEWS, Dec. 13, 2002, http://news.zdnet.com/2100-9595_22-977829.html.

50. SMART CARD ALLIANCE, CONTACTLESS PAYMENTS: DELIVERING MERCHANT AND CONSUMER BENEFITS 4 (2004), http://www.smartcardalliance.org/pdf/alliance_activities/ contactless_pmt_benefits_report.pdf [hereinafter SMART CARD ALLIANCE, CONTACTLESS

Banks and merchants are investing heavily in contactless payment technology believing it will indeed yield greater profits: "Leading banks are issuing millions of contactless credit and debit cards to consumers . . . . The rate of deployment of contactless infrastructure is the highest ever observed for emerging payments products and technology in recent memory and speaks of a unique market momentum for the industry."[51] "Ubiquitous acceptance across all merchants . . . is in process," the payment associations and bank card issuers have already joined forces, and "[m]ajor milestones have already occurred."[52] Contactless payment systems will soon be a part of everyday life.[53]

II. THE PRIVACY LANDSCAPE

RFID proponents have recognized the lack of focus by privacy advocates regarding the potential dangers of RFID applications:

> Policy and process leaders in government and business, as well as the various think tanks, have not really gotten a handle on the impacts all these pervasive technologies [including RFID] will have on us going forward.
>
> . . . .
>
> . . . The law is not on your side here—your information is being shared. Mostly because of our own consumerism and desire for convenience. . . . What gave them the right? You did![54]

PAYMENTS].

51. SMART CARD ALLIANCE WHITE PAPER, *supra* note 11, at 2.

52. *Chase Defines Contactless Payments . . . and Contactless Payments Help Redefine Chase—A Conversation with Scott Rau*, CONTACTLESS NEWS, Oct. 3, 2005, http://www.contactlessnews.com/library/2005/10/03/chase-defines-contactless-payments-and-contactless-payments-help-redefine-chase-a-conversation-with-scott-rau/. Chase adds that it has "rolled out [its new 'blink' contactless payment card] in two regions, acquirers have agreed to support it, and merchants are taking it up." *Id.* As of April 2004, "[m]illions of U.S. consumers are already paying for purchases using contactless payment devices, with millions more expected this year as new financial industry-backed contactless payment initiatives are launched nationwide." SMART CARD ALLIANCE, CONTACTLESS PAYMENTS, *supra* note 50. As of September 19, 2005, Chase had issued more than two million of its blink cards. *HSBC Joins Contactless Fray*, RFID NEWS, Sept. 19, 2005, http://www.rfidnews.org/news/2005/09/19/hsbc-joins-contactless-fray/.

53. *See, e.g.*, Susan Warren, *Why Some People Put These Credit Cards in the Microwave*, WALL ST. J., Apr. 10, 2006, at A1.

54. Lucy West, *The Future: SmallSmartFast, Scary and Fun!*, CHAINLINK RES., Jan. 1, 2004, http://www.chainlinkresearch.com/research/detail.cfm?guid=F8DE5629-37E3-4BB0-BEFB-3184DC21D442.

Privacy advocates' criticisms, however, have been focused almost exclusively on two planned RFID applications: EPC tags as UPC bar code replacements in consumer products, and RFID chips in government-issued identification cards and papers. Privacy concerns caused by contactless payment systems have received little, if any, attention.

A. Very Little Static Has Been Raised Regarding Contactless Payment Systems

When plans to test EPC tags as UPC bar code replacements were first announced, privacy advocates responded with vigor, collaborating in the publication of an *RFID Position Statement of Consumer Privacy and Civil Liberties Organizations* (*RFID Position Statement*) in November 2003.[55] The *RFID Position Statement* identified five broad privacy concerns.[56] First, RFID tags could be "embedded into/onto objects and documents without the knowledge of the individual who obtains those items."[57] Second, each RFID tag produced would have a unique EPC, which could allow every physical object to be "identified and linked to its purchaser or owner at the point of sale or transfer."[58] Third, "massive databases" containing EPCs from RFID tags embedded in objects could be linked with individuals' "personal identifying data" in the future.[59] Fourth, since RFID readers have "already been experimentally embedded" in objects such as floor tiles, carpeting, and doorframes, RFID readers could also be easily hidden in places where RFID tags embedded in objects worn or carried by unsuspecting individuals could be scanned.[60] Finally, and most importantly, if

55. RFID Position Statement, *supra* note 8. The consortium included eight organizations, among them privacy advocacy heavyweights such as the ACLU, EPIC, and the EFF. The Center for Democracy and Technology (CDT) is a prominent endorser, and many other organizations and experts have also endorsed the statement.

56. *Id.* Each of the five identified concerns does not expressly focus on EPC tags as UPC bar code replacements, but each statement does appear rooted in the paradigm that RFID-enabled microchips will only be embedded in non-human objects and be used chiefly as replacements for UPC bar codes. *See, e.g.*, Katherine Albrecht, *Supermarket Cards: The Tip of the Retail Surveillance Iceberg*, 79 DENV. U. L. REV. 534, 561–62 (2002) (asserting RFID is a "consumer goods tracking system" in which EPC tags appear "in every store-bought item in a consumer's home"); *see also* EFF, Radio Frequency Identification (RFID), http://www.eff.org/Privacy/Surveillance/RFID/ (last visited Dec. 22, 2006) (asserting RFID is "a convenient way to . . . track people and their activities through their belongings").

57. RFID Position Statement, *supra* note 8.

58. *Id.*

59. *Id.*

60. *Id.*

"personal identit[ies] were linked with [EPCs,] . . . individuals could be profiled and tracked without their knowledge or consent."[61]

Privacy advocates have raised significant static about the potential for EPC tags embedded in consumer products to create a surveillance infrastructure and, to some extent, have warned of privacy concerns caused by government-issued identification cards featuring RFID technology.[62] Despite these broad statements of concern, privacy advocates have not drawn meaningful attention to privacy concerns caused by contactless payment systems. The banks and merchants pushing contactless payment systems have not acknowledged that their systems intrude on individuals' privacy either. Banks and merchants

61. *Id.*

62. *See* Albrecht, *supra* note 56, at 562 (mentioning without elaboration that RFID "applications could include shopping carts that automatically bill consumer's accounts" and focusing the attention of the Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN) on fighting the global adoption of EPC tags as UPC bar code replacements in consumer products); *RFID: Privacy Advocates Question Retailers on Goals of 'RFID' Tracking Technology*, Privacy L. Watch (BNA), at D-2 (June 14, 2004) (quoting the EFF's Tien's assertion that "we have to think about policy issues" when consumers start "bringing home items with [EPC tags] . . . attached to them," but recognizing no privacy concerns caused by contactless payment devices even when consumers make no purchases of EPC-tagged consumer products, or that contactless payment devices may be used either to purchase things with no EPC tag attached or things not brought home, such as a meal at a restaurant or a movie admission ticket); *see also* Bill Christenson, Veripay Credit-Card Implant: Science Fiction in the News (Nov. 27, 2003), http://www.technovelgy.com/ct/Science-Fiction-News.asp?NewsNum=20 (quoting Beth Givens of the PRC that "a robust credit card network based on RFID chips implanted under the skin" would create an infrastructure for government surveillance, but reporting no comment by Givens that would indicate Givens recognized contactless payment devices in any form factor create the same surveillance infrastructure capability); Beth Givens, Dir., PRC, Testimony Before the Cal. Leg. J. Comm. on Preparing Cal. for the 21st Century: RFID and the Public Policy Void (Aug. 18, 2003), http://www.privacyrights.org/ar/RFIDHearing.htm [hereinafter Givens, RFID Public Policy Void] (mentioning credit cards among a long list of objects that could be "located and read at a distance" using RFID, but recognizing no privacy concerns so long as "businesses use smarter privacy-protective RFID technology than is in use today in . . . ExxonMobil's SpeedPass"); Tien, *supra* note 10 (focusing attention on RFID-enabled, government-issued identification cards). EPIC notes that Applied Digital's VeriPay system "raises the same privacy issues as [EPC tags,]" but does not articulate any privacy concerns with contactless payment devices in other form factors. EPIC VeriChip Page, http://www.epic.org/privacy/rfid/verichip.html (last visited Dec. 22, 2006). It is noteworthy that the only mention of the terms "contactless" and "smart chip" in the PRC's online archives are in a posting entitled "RFID Implementation in Libraries." *See* Beth Givens, Dir., PRC, Presentation to American Library Association: RFID Implementation in Libraries: Some Recommendations for "Best Practices" (Jan. 10, 2004), http://www.privacyrights.org/ar/RFID-ALA.htm; Lee Tien, Staff Att'y, Presentation to American Library Association: RFID and Libraries: EFF Talking Points for ALA IFC (Jan. 10, 2004), http://www.privacyrights.org/ar/RFID-ALA.htm.

only appear to be concerned with solving fraud-related security issues[63] and, in that context, assert that contactless payment devices should be less susceptible to fraud than plastic cards.[64] However, security and privacy are different things. Security enables banks, merchants, and consumers to protect their money from theft. Privacy, in general terms, is about allowing individuals to control the disclosure of their nonpublic personal information. Addressing security problems in contactless payment systems and devices does not address the privacy problems caused by contactless payment systems. Outside the circle of banks and merchants pushing contactless payment systems, no other RFID proponents are actively discussing privacy concerns caused by contactless payment systems. Whatever the cause of this lack of attention to the privacy problems caused by contactless payment systems, the privacy problems are numerous and significant.

B. What Privacy Problems Are Caused by Contactless Payment Systems?

1. Security Flaws Cause Privacy Problems

Unlike the passive RFID microchips used in EPC tags, which can be embedded without consumers' knowledge or consent and could be difficult, if not impossible, for consumers to detect or locate, individuals carrying contactless payment devices know the precise location of the smart chip in their devices and have tacitly consented to carry it. Precise knowledge of the smart chip's location, coupled with the flawed perception that a contactless payment device must be brought within inches of a reader to be interrogated, could lead individuals to believe they can control any RFID reader's ability to interrogate their contactless payment device and may explain why privacy advocates are not more vocal about surreptitious tracking of contactless payment devices.[65] However, "radio-frequency transmissions" are by their very nature "physically insecure,"[66] and at least one test has shown that the low-frequency passive RFID devices popular in contactless payment devices in the United States can be read from "far greater distances than

63. *See infra* notes 80–95 and accompanying text.

64. *See infra* notes 68–69 and accompanying text.

65. Evan Schuman, *How Safe Are the New Contactless Payment Systems?*, EWEEK, June 20, 2005, http://www.cioinsight.com/print_article2/0,1217,a=154404,00.asp [hereinafter Schuman, *Contactless Payment*]; *see also* SMART CARD ALLIANCE WHITE PAPER, *supra* note 11.

66. Tien, *supra* note 10, at 3.

[the two to four-inch read range that] vendors claim."[67] Chase asserts that this distance-based threat is irrelevant because its new blink cards contain other built-in security measures,[68] "including 128-bit and triple [Data Encryption Standard (DES)] encryption" plus a cryptogram that changes with every transaction.[69] Chase's assertions are not without flaws.

First, not all contactless payment devices feature such advanced encryption. The Texas Instruments Digital Signature Transponder

67. Schuman, *No-Touch Retail*, *supra* note 13. Shell Canada conducted a test using a high-power antenna, the kind it "believe[s] thieves would use," on "[t]he kind of low-frequency [passive RFID] tags popular in the United States" in contactless payment devices, and found that these tags could be compromised and read from a distance of about ten meters. Schuman, *Contactless Payment*, *supra* note 65. In fact, "[a]ny compatible reader within range of the . . . [contactless payment device] could read [any] . . . data" stored on the device. Tien, *supra* note 10, at 4. Recent demonstrations by researchers from the University of Massachusetts prove this point. *See* Weston, *supra* note 37.

68. SMART CARD ALLIANCE WHITE PAPER, *supra* note 11. Similar to Chase's assertion of other built-in security measures, the Smart Card Alliance's Contactless Payments Council (Payments Council) asserts that "contactless payment technology . . . is built from the ground up on requirements for high security" using "sophisticated smart chip technology with built-in intelligence and multiple safeguards specifically designed to protect against fraud." *Id.* at 3. The Payments Council never identifies the "other" security measures it asserts exist but does appear to identify the true source of these "other" security measures: "[b]uilt on the *current payment infrastructure*, contactless payments leverage layered security systems." *Id.* (emphasis added). The *current* payment infrastructure touted by the Payments Council cannot guarantee security as evidenced by the fact that fraud losses on credit and debit cards in the United States grew from $2.37 billion in 2003 to $2.66 billion in 2004—and are projected to reach $3.21 billion in 2007. ePaynews.com, Payment News and Resource Center, Statistics for General and Online Card Fraud, http://www.epaynews.com/statistics/fraud.html#21 (last visited Dec. 22, 2006). MasterCard admits that its new PayPass contactless payment device merely "increases [its customers'] *feelings* of security, since they remain in control of their cards during all transactions." *MBNA America Bank Launches Contactless Credit Cards in Atlanta*, CONTACTLESS NEWS, Oct. 17, 2005, http://www.contactlessnews.com/news/2005/10/17/mbna-america-bank-launches-contactless-credit-cards-in-atlanta/ (emphasis added). MasterCard does not make the same broad, "layered security" claim asserted by the Payments Council, and if we accept MasterCard's statement as true that only its customers' "feelings" of security are enhanced by contactless payment devices, then such devices will remain exposed to the same sources of fraud that have plagued card-based payment methods since their introduction. As Oliver Steeley, MasterCard International's vice president of wireless payment devices, admits, "Contactless cards are safer in some ways and riskier in others, but overall, the new model appears to be a security wash." Schuman, *No-Touch Retail*, *supra* note 13.

69. Schuman, *Contactless Payment*, *supra* note 65. "Triple DES is a block cipher formed from the Data Encryption Standard (DES) cipher by using it three times." Wikipedia, Triple DES, http://en.wikipedia.org/wiki/Triple-DES (last visited Dec. 22, 2006). Triple DES is a simple way to enlarge the 56-bit key of the Digital Encryption Standard (DES) to guard against brute force attacks without having to switch to a new algorithm. *Id.*

(DST) used in the ExxonMobil Speedpass key fob[70] features a forty-bit, unpublished, proprietary key that a research team cracked and used to clone a device capable of completing fraudulent gasoline purchase transactions at ExxonMobil stores.[71] Second, despite the privacy and security promised when encrypted security keys and cryptographic processes are manufactured into contactless payment devices—including the high-level encryption Chase claims would render any data improperly captured from its blink cards useless[72]—any encryption security "scheme is not absolute" when "[t]here is no cardholder verification (i.e.[,] a signature or a PIN)."[73] Patrick Gauthier, senior vice president for emerging products development at Visa, one of Chase's partners in the blink card project, admits that even when factoring in 132-bit and triple DES encryption, "[a] thief that scanned the [blink card] . . . would be able to capture the credit card number"[74] stored in the device.

Finally, encryption keys cannot, by themselves, guarantee data security. Lee Tien of the Electronic Frontier Foundation (EFF), speaking in the context of RFID-enabled, government-issued identification cards, identified a number of privacy-threatening weaknesses with encryption security.[75] First,

> [e]ven if [all] the data stored . . . [in a contactless payment device] is encrypted, an enormous number of authorized users . . . would be in a position to abuse their authorized access

70. "More than 6 million *Speedpass* devices have been issued in the U.S." Speedpass Fact Sheet, http://www2.exxonmobil.com/corporate/files/corporate/speedpass_fact_sheet.pdf (last visited Dec. 22, 2006).

71. Bono et al., *supra* note 27, at 2.

72. Schuman, *Contactless Payment*, *supra* note 65.

73. Birch, *supra* note 11 (emphasis omitted).

74. Schuman, *Contactless Payment*, *supra* note 65. As an example:

> [R]ecently, two researchers at the University of Massachusetts pulled unencrypted names, account numbers and expiration dates off contactless credit cards using a homemade scanning device.
>
> . . . [O]ne of the UMass researchers, Tom Heydt-Benjamin, was able to buy electronic equipment online using information pulled off a contactless card [while the card was] sealed inside an envelope.
>
> The "Today" show aired footage demonstrating another data capture, in which Heydt-Benjamin concealed the scanner in a briefcase and "read" data from a contactless credit card in another person's back pocket.
>
> . . . [A]nyone with the right equipment can read the data, and the equipment needed to do so is getting cheaper and more sophisticated all the time.

Weston, *supra* note 37.

75. Tien, *supra* note 10, at 7–8.

> to the data. If the data were read directly from the cards themselves . . . it would be difficult to maintain an audit trail . . . and therefore very difficult to detect abuse.[76]

Second, even if all the data stored in a contactless payment device is encrypted, "an attacker could eavesdrop on a legitimate data transmission between the [contactless payment device] and the RFID reader."[77] Third, "[b]y definition, every authorized RFID reader can decrypt the data stored [in contactless payment devices] [t]hus many thousands of readers would have access to the keys needed to read the [contactless payment devices]," and it would be "essentially impossible to maintain the confidentiality of such widely distributed information."[78] Fourth, and ominously,

> encryption cannot solve the [surreptitious] tracking problem because encrypting unique information will result in different, but still unique, information.
>
> . . . .
>
> . . . So long as *any* unique identifier is readable without additional safeguards, neither encryption nor PIN-based access control protects against tracking. If an identifying number is available, it can be used to track the card's movements, and then later used to link the card to the holder's identity. Even if the *entire* contents of the chip are encrypted, it remains trackable; the encrypted data block itself provides a unique identifier.[79]

Beyond encryption, critics assert that the few suggested privacy-related security measures are either ineffective or are too expensive. Moreover, the few suggested measures also work to defeat banks' and merchants' transaction speed and convenience goals for contactless

---

76. *Id.* at 7.

77. *Id.*

78. *Id.* Tien provides an illustration:

> If every card is protected by the same encryption key or [PIN,] . . . then each [authorized] reader would need to have that PIN or key . . . . Researchers have successfully extracted PINs from supposedly secure smart cards and successfully extracted encryption keys from stolen card readers. Once the system has been compromised, "bootleg" readers could easily be created. One might also steal the PIN or key from inside the system. Storing the key in, say, an attached computer system, rather than in the reader hardware itself, makes this attack easier, not harder. The computer is just as easy as the reader to steal, and generally easier to extract the key from. Over time, the result would be essentially the same as not using a PIN and not encrypting the data. It is hard to imagine how the system would recover from this sort of breach.

Id.

79. *Id.* at 8.

payments. MasterCard, for example, suggested that a password requirement may be the answer.[80] One disadvantage of requiring a password is that it introduces a manual, time-consuming component into transaction processing because a password, like a PIN, must be manually keyed or otherwise manually transmitted into a POS terminal. Moreover, requiring a password would cause transaction processing time to be significantly increased, if not doubled. This is because passwords, like PINs, may need to be authenticated in a separate "transaction" prior to the payment authorization transaction. In other words, two sets of communication transmissions might be required between the POS terminal and the host to complete one payment transaction. Passwords, like PINs, would also be susceptible to decryption by thieves using encryption keys from stolen readers. From a practical standpoint, unless passwords are stored in the contactless payment device, passwords, like PINs, could also be compromised by thieves standing close enough to see, overhear, or otherwise intercept a password given during a transaction. The thief could then steal the victim's contactless payment device and exploit it until the issuer is contacted to deactivate the device or the affected account.

ExxonMobil recently introduced "Zip Code Verification" at its fuel dispensers and its in-store POS terminals to help protect its customers against fraudulent use of Speedpass devices.[81] Like passwords and PINs, the need to key-enter a zip code introduces a manual, time-consuming component into the transaction-approval process since the zip code must be manually keyed and would likely need to be authenticated in a separate transaction prior to the payment transaction. Thieves standing nearby could also watch a customer enter his or her zip code and would otherwise be able to make fraudulent transactions by stealing both the device and the customer's wallet, which likely contains a driver's license, for example, complete with a zip code printed on its face.

Another suggestion involves fitting contactless payment devices with a "switch to make or break the connection between the chip and antenna, [allowing] the cardholder [to] squeeze the switch to turn on the card and wave it before a reader to make payments."[82] The idea behind this feature is to prevent a device from being scanned by an RFID

80. Schuman, *No-Touch Retail*, *supra* note 13.

81. Speedpass: My Account, New Zip Code Verification—For Your Protection, https://www.speedpass.com/forms/frmDynPage.aspx?pPg=ZipVerification.htm&pgType=N (last visited Dec. 22, 2006).

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

reader unless the device's switch has been squeezed on.[83] Such a solution adds a manual step to transaction processing, making the use of the device less convenient, and this inconvenience would be further compounded if a customer had difficulty activating the switch or the switch failed. Moreover, such a system would not defeat a thief's use of a high-powered antenna[84] or eavesdropping attack to access any data stored on the device while the device is switched on.

Finally, biometric authentication[85] provides a possible solution, but critics assert that the costs to implement biometric authentication systems are, at present, too expensive to justify their benefit.[86] In addition, biometric authentication systems insert a manual step into the transaction process because the biometric identifier must be manually transmitted to the POS terminal. Like passwords, requiring a biometric authentication could significantly increase, if not double, transaction-processing time. Further, "[n]o biometric [authentication] method is foolproof—identity can be forged in a variety of ways. . . . If someone compromises your fingerprint or voiceprint profile, your profile can never be truly secure again."[87]

Even if contactless payment device issuers implement a password, on-off switch, or biometric fraud prevention system, such devices would only provide security at the point-of-sale. Identity thieves can moot the effectiveness of password or biometric-based security systems by using pretexting,[88] social engineering,[89] phishing,[90] or pharming[91] scams to

83. *Id.*

84. *See* Schuman, *Contactless Payment*, *supra* note 65.

85. Biometric authentication refers to technologies that primarily measure and analyze for authentication purposes such physical characteristics as "fingerprints, eye retinas and irises, facial patterns and hand measurements," and possibly even voiceprint profiles. *See* Wikipedia, Biometrics, http://en.wikipedia.org/wiki/Biometrics (last visited Dec. 22, 2006).

86. Paturi, *supra* note 82.

87. Gregory Anderson, *Hello Me, It's Me Again: The State of Biology-Based Security*, SMART COMPUTING, Aug. 2005, at 44.

88. Pretexting usually involves a person pretending to be a customer contacting a bank or merchant and lying or using deception in order to trick the bank or merchant into giving up a customer's nonpublic personal information. *See* Wikipedia, Social Engineering (Security), http://en.wikipedia.org/wiki/Pretexting (last visited Dec. 22, 2006).

89. Social engineering, in this context, involves "obtaining confidential information by manipulation of legitimate users," usually by a person using a telephone or the Internet to exploit individuals' natural tendency to trust others and thereby tricking individuals into revealing, inter alia, nonpublic personal information. *See* Social Engineering: Information from Answers.com, http://www.answers.com/topic/social-engineering-security (last visited Dec. 22, 2006).

90. Phishing involves:

criminal activity using social engineering techniques. Phishers attempt to

obtain sufficient authentication information from a victim and then, for example, contact the device's issuer to have a contactless payment device sent to the thief's own address. Alternatively, a thief could obtain multiple individuals' nonpublic personal information by hacking into a credit issuer's databases or by working with "insiders with knowledge of and access to the system"[92] and then, for example, contact a device's issuer to have a contactless device sent to the thief's own address.[93]

In sum, the security solutions proposed by banks and merchants will do little, if anything, to allay privacy concerns arising from the security problems inherent in any contactless payment system, especially given the frequency of massive losses of individuals' nonpublic personal information due to fraud, mistake, or other cause.[94] It appears that the issuers of contactless payment devices can only offer consumers one consolation: if a customer's contactless payment device is stolen or unauthorized charges are otherwise made to his or her account, the issuer will not hold the customer liable.[95] Such a concession merely

> fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an electronic communication. Phishing is typically carried out using email or an instant message, although phone contact has been used as well.

Wikipedia, Phishing, http://en.wikipedia.org/wiki/Phishing (last visited Dec. 22, 2006).

91. Pharming involves exploiting vulnerabilities in Domain Name System (DNS) software, allowing a hacker to hijack the domain name, for example, of a bank or merchant, and redirect the bank's or merchant's Web site traffic to a bogus site set up for the purpose of "obtain[ing] access credentials such as usernames and passwords." *See* Wikipedia, Pharming, http://en.wikipedia.org/wiki/Pharming (last visited Dec. 22, 2006).

92. Tien, *supra* note 10, at 2.

93. For a comprehensive list (of at least reported cases as of April 20, 2006) of the means by which identity thieves have successfully gained access to individuals' nonpublic personal information, see PRC, A Chronology of Data Breaches Since the ChoicePoint Incident, http://www.privacyrights.org/ar/ChronDataBreaches.htm (last visited Dec. 22, 2006).

94. The frequency of security breaches in which identity thieves gain access to massive numbers of individuals' nonpublic personal information does not appear to be slowing since the ChoicePoint debacle, "a watershed event in terms of disclosure to the affected individuals," was made public on February 5, 2005. *Id.* In the fourteen-month period following the ChoicePoint incident, 156 security breaches affecting a total of 54,830,477 individuals were reported in the United States alone. *Id.* The number of actual identity thefts in 2005 was a lower number: 255,565 cases of identity theft were reported through the FTC's Sentinel system in 2005. *See* FED. TRADE COMM'N, *supra* note 21, at 4. One can only wonder how many others have simply not yet discovered they are victims.

95. *See* Schuman, *Contactless Payment*, *supra* note 65 (reporting that Chase's new blink cards feature "several security factors, including Chase's 'zero liability policy,' which protects consumers but not necessarily the retailers").

restates what credit and debit account issuers already do, and it adds nothing to compensate individuals whose privacy rights are violated by identity thieves.

Subdermal RFID seems to be the inevitable solution to mitigate security problems that cause threats to privacy. Contactless smart chips embedded subdermally in humans would make the device impossible for the rightful holder to lose and rather difficult (and barbaric) for a thief to steal.[96] Assuming subdermal contactless payment devices feature 128-bit and triple DES, or higher, encryption for all data stored on the subdermal chip, an individual's subdermal contactless payment device would be difficult for all but the most resourceful identity thieves to exploit as a source for obtaining a person's nonpublic personal information.[97] In addition, even if a thief obtained from other sources all the information he or she needed to steal an individual's identity, device issuers could refuse to issue a contactless payment device unless the customer appeared in person to have a subdermal contactless device with a correct cryptogram implanted in his or her arm or hand—meaning a device issuer could require whatever personal information it wanted of its "implantees" in order to authenticate each customer's identity, making it even more difficult for identity thieves to succeed in their schemes.[98] That it is difficult does not, however, mean that it is impossible. Issuers of contactless payment devices would still need to be wary of identity thieves with insider contacts with access to reset a

96. Although wearable or pocketable contactless payment devices are not fraud-proof because they can easily be lost, stolen, or obtained by thieves who open fraudulent accounts using stolen identities, *see, e.g.*, Paturi, *supra* note 82, Applied Digital asserts that its subdermally implantable VeriChip "cannot be lost, stolen, misplaced, or counterfeited." VeriChip Corporation, Solutions, http://www.verichipcorp.com/solutions.html (last visited Dec. 22, 2006). Applied Digital may not have had the stomach to recognize that a thief bent on stealing a subdermal contactless payment device might not be deterred by the need to extract a subdermal contactless payment device from his victim's arm or hand.

97. *See supra* notes 70–79 and accompanying text.

98. One possibility is that the issuer could ask a series of random, "non-wallet" questions, similar to those currently used by credit bureaus when giving persons access to credit reports over the Internet. For example, before releasing a credit report ordered online, Equifax asks a series of "non-wallet" questions to authenticate the customer's identity. "Non-wallet" questions are those for which answers are not likely carried in an individual's wallet or purse but are based on information contained in the customer's credit file and, thus—theoretically—knowable only by the person whose credit report is being accessed. *See, e.g.*, Equifax Business Solutions, Online Privacy Policy & Fair Information Principles, http://www.equifax.com/universal/privacy.shtml (lasted visited Dec. 22, 2006) (stating definition in the "Notice" section); Equifax Personal Solutions: Credit Reports, Credit Scores, Protection Against Identity Theft, http://www.equifax.com/ (last visited Dec. 22, 2006).

cryptogram in an issuer's database to match the cryptogram in a cloned subdermal device. They would also need to be on guard against identity thieves who are able to obtain sufficient nonpublic personal information on their victims to show up at the issuer's location and successfully dupe the issuer into issuing a valid subdermal contactless payment device. Finally, even if subdermally implanting contactless payment devices reduces device theft, banks and merchants would still have to contend with other major data security problems.[99] Since contactless payment device security cannot be guaranteed, individuals' privacy cannot be guaranteed.[100]

99. Data security is, indeed, a major problem. While the actual number of identity theft complaints received each year by the FTC is a much lower number, *see* FED. TRADE COMM'N, *supra* note 21, at 6, the "Federal Trade Commission estimates that more than 10 million Americans are victims of such crimes annually, costing individuals $5 billion and businesses $48 billion." Karim Toubba, *Fighting Data Theft*, LINE56, July 19, 2005, http://www.line56.com/articles/default.asp?articleid=6727. Toubba points out that in each of the massive data thefts in early 2005 from BJ's Wholesale Club, Polo Ralph Lauren, Bank of America, Citibank, DSW Shoe Warehouse, CardSystems, and Lexis-Nexis, "the nature of the vulnerability exploited was different, ranging from misplaced backup tapes and unpatched servers to hackers accessing important data and many other flaws." *Id.* Toubba argues that "no single technology [including RFID] . . . can safeguard retailers against these varied risks; however, more rigorous security training and policies, more robust authentication, and better controls over outsourcing entities will all play critical roles in ensuring that critical data remains secured." *Id.* In addition, the data security problem is not limited to just the internal, back-office variety. For example, assuming multiple banks eventually choose to adopt and issue subdermal contactless payment devices, individuals will not want to be implanted with a separate subdermal chip from every credit, debit or other payment account issuer they do business with. Such consumer resistance would create the need for a single subdermal chip accessible by multiple credit, debit or other payment account issuers and by all merchants who accept those issuers' payment methods. This need for shared access among banks and merchants would seem to increase an identity thief's odds of success due largely to the increased number of potential data security attack points. Worse, if a portion of a subdermal chip's memory was reserved for nonpublic personal identification information accessible by all banks, an identity thief's odds of success could be even greater because the thief would only need to access the chip to compromise the victim's privacy. Moreover, if contactless payment device issuers ever report their devices' EPCs along with their customers' other nonpublic personal information to data compilation companies such as ChoicePoint or credit bureaus such as Equifax, one internal data security breach could have far-reaching consequences. Based on the frequency and variety of the reported data security breaches, none of these concerns can be casually dismissed. *See supra* notes 93–94 and accompanying text.

100. There is a feature of active RFID technology that should concern privacy advocates: active RFID technology can be leveraged to make contactless payment devices do double-duty as RFID readers by using NFC technology. Birch, *supra* note 11. Although most contactless payment devices currently operate on passive RFID technology, future generations of contactless payment devices may feature either active RFID microchips, microchips capable of operating in both active and passive modes, or even multiple passive and active RFID-enabled microchips handling separate functions. The subdermally-

2. "Big Bucks"—Privacy Rights Take a Back Seat to Profits

In addition to their desire to increase transaction speed and convenience for customers, banks and merchants are interested in maximizing the return on their investment in contactless payment systems by leveraging data gained from customer contacts and transactions.[101] As the numbers of data collection points and the types and amounts of customer data increase, data security will become much more important. In tandem with increased data collection, customers will enjoy increased conveniences, but as customers demand more and greater conveniences, their privacy may shrink in direct proportion. IBM's "Margaret" project provides an illustration:

> IBM has figured out a way to use RFID to help banks and other organizations to identify individual customers . . . .
>
> The system involves embedding a UHF RFID tag in a passbook or loyalty card. When a customer enters the bank, the tag is scanned automatically and the person is identified. . . .

implantable VeriChip used in Applied Digital's VeriPay system illustrates one current use of active, low-frequency RFID smart chips in contactless payment devices. *See* VeriChip Corporation, *supra* note 96. NFC, which is billed as the "next generation of standards" in RFID, will permit devices such as mobile phones and PDAs, which have their own onboard power sources, to function as passive RFID contactless payment devices when their power is turned off or their battery is dead. Birch, *supra* note 11. But when the mobile phone or PDA's power is turned on, the device would be capable of acting as an active RFID device, thus enabling it to act as a POS terminal to accept contactless payments from any other contactless payment device, including other powered-off mobile phones or PDAs. *Id.* In addition to mobile phones and PDAs, iPods, Gameboys, or other hand-held electronic devices could double as both contactless payment devices and innocuous-looking RFID readers, giving every person in possession of such a device a tool to surreptitiously read the EPC, credit, debit, or other account number, and any other nonpublic personal information stored on *any* contactless payment devices, as well as the EPC on any tagged consumer product or on any RFID-enabled identification card. Lee Tien of the EFF reports:

> RFID reading devices are easy to build, and will be easier to build as RFID technology spreads. Nokia last year unveiled a cell phone that can read RFID tags . . . . There already exist SD cards for Palm-compatible handhelds that can convert popular PDAs like the Treo into RFID readers . . . . German hacker Lukas Grunwald used his RFDump software on a PDA equipped with an RFID reader to read and write to RFID tags in a German grocery store.

Tien, *supra* note 10, at 3 (citations omitted).

101. *See supra* notes 47–52 and accompanying text; *see also* John Stermer, *Radio Frequency ID: A New Era for Marketers?*, CONSUMER INSIGHT MAG., Winter 2001, *available at* http://web.archive.org/web/20020210070506/http://acnielsen.com/pubs/ci/2001/q4/features/radio.htm ("RFID enables the linking of . . . product information with a specific consumer identified by key demographic and psychographic markers. . . . [N]ow we can correlate multiple points of consumer product purchase with consumption specifics such as the *how*, *when* and *who* of product use.").

> . . . [T]he system can be linked to a bank's customer relationship management software, where personal information is stored, including how the person like's [sic] to be addressed and a history of [his or her] recent interactions with the bank.[102]

"Margaret" illustrates the types of privacy problems that could accompany contactless payment systems and, particularly, subdermal contactless payment systems.

First, wearable or pocketable contactless payment devices will not deter thieves. Thus, in searching for viable security solutions, banks and merchants will likely recognize that subdermally-implanted contactless payment devices could provide the means to reduce fraud significantly.[103] Second, to make marketing programs like "Margaret" work in an environment where contactless payment devices are purported to have very short interrogation ranges, banks or merchants must either use powerful RFID readers to identify customers from a distance or must embed contactless payment devices with a second, high-frequency RFID tag which could be interrogated from a greater distance. Third, when customers become accustomed to the convenience offered by marketing programs like "Margaret" at all the banks and merchants with whom they do business, it would likely be easier to convince customers of the convenience of a single contactless device readable by every bank or merchant, as opposed to a thick wad of plastic cards or a pocket full of key fobs. Banks and merchants are likely to recognize that when consumers' demand for convenience is combined with the better fraud protection offered by subdermally-implanted contactless payment devices, a "one-subdermally-implanted-contactless-payment-device-fits-all" solution will be difficult to ignore.[104] Even if subdermal contactless payment systems are neither adopted for widespread use nor leveraged for other purposes, the development of near-field communication (NFC) technology indicates that banks and merchants may be likely to employ RFID-enabled microchips that operate, singly, in both passive and active modes—or perhaps both low-

102. *RFID May Boost Service at Banks*, RFID J., Apr. 25, 2003, http://www.rfidjournal.com/article/articleview/396/1/20/; *see also* Peter Wray, *Building Loyalty in a Disloyal World*, COLLOQUY, 2004, https://www.colloquy.com/online/past_issues/v12i1/v12i1tpbuilding.asp ("Only companies that understand their customers better than their competitors do are very likely to survive. . . . To truly understand me as a customer, you must . . . [i]dentify me . . . [and] [t]rack what I buy . . . .").

103. There is one sizeable caveat. *See supra* note 99.

104. Banks and merchants would still need to address data security since data stored in and transmitted by contactless payment devices is not secure even when encrypted. *See supra* notes 75–79 and accompanying text.

and high-frequency RFID microchips—in the wearable or pocketable contactless devices they issue to achieve their marketing goals. In such a scenario, consumers would expect the presence of a low-frequency RFID smart chip in their contactless payment device, even though they would not likely know it by its technical name, because that is what makes the device work. However, many consumers might not understand the significance of the presence of both a low-frequency smart chip and a high-frequency, passive EPC tag—or both passive and active RFID smart chips—in their contactless payment devices. Even if customers were made aware of the presence of multiple RFID tags or smart chips in their contactless payment devices, customers would not attempt to locate and disable them for fear of destroying their device's payment functionality. Thus, contactless payment devices could conceivably become readable from great distances by virtue of a ride-along, high-frequency EPC tag. Even if no high-frequency RFID tag was used, the low-frequency smart chip could still be read from a distance with high-power antennae or still be subject to eavesdropping attacks. Fourth, regardless of the numbers or types of RFID-enabled microchips used in contactless payment devices, the concerns of privacy advocates about the surreptitious tracking of individuals by EPC tags embedded in consumer products would be a moot issue. It would be of no consequence whether individuals could be tracked by EPC tags embedded in, for example, their clothing or shoes because their contactless payment devices, assuming they are usually present and never transferred to other persons, provide the optimal devices for banks and merchants to exploit in gaining intelligence about their customers—or for thieves to victimize unsuspecting individuals. Taken together, and combined with the vacuous privacy policies of most banks and merchants,[105] there is great cause for concern.

3. "Big Brother"—Significant Moves Toward Involuntary Surveillance

Governments worldwide have already begun to use both passive and active RFID microchips for a variety of purposes. In the United States, the Department of Defense mandated that its suppliers provide passive RFID tagging on "all freight/cargo containers, cases, pallets and to individual 'high-value' items that require the military's UID (Unique Identification Code)."[106] The Department of Defense also mandated

105. *See infra* notes 189–201 and accompanying text.

106. RFID 101: RFID and DoD Policy, http://www.rfid-101.com/rfid-dod.htm (last visited Dec. 22, 2006) [hereinafter RFID and DoD Policy]; *see also* Grant Gross, *RFID and*

that "[c]ontainers shipped outside the continental US [sic] need to have active [RFID] tags with content and point of origin information."[107] The Department of Homeland Security implemented its "Visa Waiver Program" featuring "e-Passports" on October 26, 2006.[108] The Department of Homeland Security also considered plans for RFID-based identification cards to be used at border crossings.[109] Presumably, these applications, should they actually materialize, will make use of low-frequency RFID microchips due to the high need for security, although federal lawmakers could conceivably mandate that both low-frequency smart chips and high-frequency EPC tags be embedded in the same device, whether carried, worn or even implanted subdermally, in order to track individuals' movements within the longer read ranges possible with low-frequency RFID microchips. But perhaps the largest step in the direction of a surveillance society in the United States centers on the recent passage of the Real ID Act and the seemingly inevitable conclusion that subdermal contactless devices would provide a more secure means of identification than cards worn or carried by individuals.[110] The United States government would not be the first government in North America to reach this conclusion: the Mexican government has already implanted active RFID chips into workers' arms as a means of securing access to restricted areas.[111]

Privacy advocates' assertions about the potential uses for RFID technology are replete with fears that RFID tags will become a true "über-bug."[112] For example, privacy advocates charge that governments may use RFID to track and profile individuals by such things as "matching customers' purchases against computer databases . . . [and]

Privacy: Debate Heating Up in Washington, INFOWORLD, May 28, 2004, http://www.infoworld.com/article/04/05/28/HNrfidprivacy_1.html.

107. RFID and DoD Policy, *supra* note 106.

108. U.S. DEP'T OF HOMELAND SEC., VISA WAIVER PROGRAM TRAVELER GUIDE (2006), *available at* http://www.dhs.gov/xlibrary/assets/vwp_travelerguide.pdf.

109. Jonathan Krim, *U.S. May Use New ID Cards at Borders*, WASH. POST, June 5, 2004, at E01.

110. *See, e.g.*, Declan McCullagh, *FAQ: How Real ID Will Affect You*, CNET NEWS.COM, May 6, 2005, http://news.com.com/FAQ+How+Real+ID+will+affect+you/2100-1028_3-5697111.html.

111. *See* Will Weissert, *Microchips Implanted in Mexican Officials*, MSNBC.COM, July 14, 2004, http://www.msnbc.msn.com/id/5439055/.

112. Kobelev, *supra* note 32, at 331. By "über-bug," Kobelev appears to mean "super-bug": "RFID technology has the potential to . . . lead[] to a world in which our physical location is never safe from the prying eye of the government, companies, or a hacker. As RFID technology proliferates, it will literally surround future consumers wherever they go and whatever they do." *Id.* at 330–31.

tracking a person's physical location."[113] Katherine Albrecht and Liz McIntyre allege that the United States "government plan[s] to order RFID chips embedded in all cars sold in America," which would allow "police [to] . . . track your comings and goings by putting inexpensive RFID readers at key intersections."[114] However, no privacy advocate appears to consider that governments could track and profile individuals by interrogating individuals' contactless payment devices.[115]

Regardless of the reason for the lack of dialogue on privacy issues caused by contactless payment systems, the public will not be best served by having such privacy issues addressed after contactless payment devices are widely distributed and used. The public would be best served by reasoned, careful analysis of the issues now. The Supreme Court has already ruled that individuals cannot refuse to identify themselves when government agents demand that they disclose their identity.[116] Since it is the "involuntary nature of a government mandate . . . [that would make such a mandate] particularly dangerous"[117] to individuals' privacy rights, privacy issues caused by contactless payment systems should be addressed now. Otherwise, contactless payment devices—with the aid of a little function creep and widespread distribution—could serve as a proxy for the secured form of identification mandated by the Real ID Act.[118] Unfortunately, the discussion of privacy concerns with all types of RFID applications appears to have lost traction at both the federal and state level.

C. The Giant Sucking Sound Is the Public Policy Vacuum

Contactless payment systems produce privacy concerns that should be addressed by legislators at either the federal or state level because: (1) contactless payment devices are already widely distributed in several form factors and are quickly approaching ubiquity; (2) contactless

113. *Id.* at 330.

114. Hiawatha Bray, *You Need Not Be Paranoid to Fear RFID*, BOSTON GLOBE, Oct. 10, 2005, at F2, *available at* http://www.boston.com/business/globe/articles/2005/10/10/you_need_not_be_paranoid_to_fear_rfid?mode=PF.

115. Lee Tien hinted at the possibility of such government surveillance, but neither Tien nor any other privacy advocate appears to have specifically addressed the issue. *See* Tien, *supra* note 10, at 4–5, 8.

116. Hiibel v. Sixth Judicial Dist. Court, 542 U.S. 177, 187–88 (2004).

117. Jerry Brito, *Relax, Don't Do It: Why RFID Privacy Concerns Are Exaggerated and Legislation Is Premature*, 2004 UCLA J.L. & TECH. 5 (2004), http://www.lawtechjournal.com/articles/2004/05_041220_brito.pdf.

118. Real ID Act of 2005, Pub. L. No. 109-13, div. B, 119 Stat. 231, 302 (2005) (codified as amended in scattered sections of 8 U.S.C.).

payment systems could be exploited as an infrastructure for the surreptitious tracking and profiling of individuals; and (3) individuals will not disable the smart chips in their contactless payment devices, at least not those in form factors other than traditional credit or debit card plastics, because doing so would destroy their contactless payment device's utility.[119] Despite these realities, no federal or state legislation addressing the privacy concerns caused by any RFID application has been enacted. Most of the states that have considered RFID privacy legislation have only considered it in the context of EPC-tagged consumer products, and no state has considered privacy legislation directed at contactless payment systems. It now appears doubtful that concerns about RFID applications will regain sufficient momentum to be addressed at the legislative level in the near future.

1. No State Has Enacted Privacy Legislation Directed at Any RFID Application

California was one of the first states to take up RFID privacy concerns. At a California Legislature Joint Committee hearing in mid-2003 entitled *Preparing California for the 21st Century*, Beth Givens of the Privacy Rights Clearinghouse (PRC) asserted that RFID had "sprung upon the scene with little attempt so far to address its many probable adverse impacts upon society."[120] Givens warned:

> We human beings interact and surround ourselves with a huge number of objects—our clothes, the furniture and appliances in our home, the consumer electronics we use, the food we buy, our automobiles . . . [and even] credit cards . . . .
>
> Massive data bases [sic] will not only contain the unique product codes, but also personally identifying information

119. Warren, *supra* note 53. Individuals may be able to microwave a credit or debit card to "fry" an embedded contactless smart chip and still have a working credit card to use afterward because their card's magnetic stripe could still be swiped through any POS terminal's card reader. However, individuals would not "fry" their key fob, watch, or mobile phone to disable a contactless smart chip because doing so would destroy such devices' payment-method functionality. Since form factors are trending away from card plastics, the microwave, metal wallet, and other gadget-based solutions mentioned by Warren, *id.* at A1, A16, will not provide adequate security or privacy protection for users of contactless payment devices in form factors other than credit or debit card plastics. For example, FoeBud's copper bracelet with a red light that blinks when near an RFID reader, *id.* at A16, is not a viable solution because when the light blinks, it is already too late to react—the contactless smart chip would have already been interrogated. Will we reduce ourselves to carrying our mobile phones in metal sheaths, our key chains in metal-lined pants pockets, and wear wide, metal bracelets over our wristwatches?

120. Givens, RFID Public Policy Void, *supra* note 62.

> connecting us with the RFID-coded items we buy or otherwise obtain. It is this association of personal identity with the object's unique identity that will enable both profiling and location tracking.[121]

While Givens mentioned credit cards and ExxonMobil's Speedpass, she did not directly address the privacy concerns caused by contactless payment systems.[122] Instead, Givens focused on plans to replace UPC bar codes with EPC tags, recommending that California: (1) require merchants to display clearly which products contain EPC tags; (2) require merchants to disclose when, where, and why EPC tags in products are being read; (3) require that individuals be provided a means of removing or permanently disabling RFID-enabled microchips in products they purchase or otherwise obtain, including credit or debit cards; (4) require that individuals be allowed to own readers to detect and permanently disable EPC tags; (5) require that individuals be allowed access to data about themselves stored in an RFID device; (6) require stringent security in system access, database access, and data transmissions; and (7) require accountability among users of RFID technology and its resultant data.[123] These recommendations focus primarily on the use of EPC tags as UPC bar code replacements and, as a result, do not address privacy concerns caused by contactless payment devices. Regardless, Givens's privacy concerns did not ultimately move California legislators. The California Senate killed a bill[124] that would have required retail stores using EPC tags as UPC bar code replacements to either detach or destroy RFID tags before consumers left the store.[125] A bill addressing privacy concerns with RFID-enabled identification documents such as drivers' licenses and student

121. *Id.*

122. Givens's decision not to make a bigger issue of contactless payment systems is noteworthy since, just three months before, she had responded to Applied Digital's announcement of a successful field-test of a GPS-trackable, subdermal contactless device with a brief statement recognizing that such devices could be used to create a robust credit card network that could form the '"infra-structure [sic] for potential government surveillance.'" Christenson, *supra* note 62.

123. Givens, Public Policy Void, *supra* note 62.

124. *See* CAL. DEP'T OF CONSUMER AFFAIRS, 2004 LEGISLATIVE DIGEST (2004), http://www.dca.ca.gov/legis/2004/privacy.htm#sb1834 (noting the failure of S.B. 1834, 2003–2004 Leg., Reg. Sess. (Cal. 2004), sponsored by then-Senator Debra Bowen, who was elected California's Secretary of State in November 2006).

125. S.B. 1834, 2003–2004 Leg., Reg. Sess. (Cal. 2004).

identification cards[126] was placed on the inactive file where it subsequently died.[127]

Following California's lead, several other states considered privacy legislation targeted at EPC-tagged consumer products, but all the proposed bills were either killed in committee[128] or given their last rites.[129] Maryland, Virginia, and Utah considered legislation that would have required studies of privacy concerns caused by RFID technology, but none of those bills were enacted.[130] South Dakota considered legislation that would have prohibited the implantation of an RFID microchip in any person,[131] but that bill also died in committee.[132] Even if any of these bills had become law, only South Dakota's proposal to prohibit the subdermal implantation of RFID chips in humans could

126. S.B. 768, 2005–2006 Leg., Reg. Sess. (Cal. 2005).

127. *See* S.B. 768, Current Bill Status, http://info.sen.ca.gov/pub/05-06/bill/sen/sb_0751-0800/sb_768_bill_20061130_history.html (last visited Dec. 22, 2006).

128. Missouri, Nevada, New Mexico, South Dakota, Tennessee, and Utah have each killed bills targeted at EPC-tagged consumer products. *See* S.B. 128, 93d Gen. Assem., 1st Reg. Sess. (Mo. 2005); A.B. 264, 73d Gen. Assem., Reg. Sess. (Nev. 2005); H.B. 215, 47th Leg., Reg. Sess. (N.M. 2005); H.B. 1136, 80th Legis. Assem., Reg. Sess. (S.D. 2005); S.B. 699, 104th Gen. Assem., Reg. Sess. (Tenn. 2005); S.B. 867, 92d Gen. Assem., 2d Reg. Sess. (Mo. 2004); H.B. 251, 55th Leg., Gen. Sess. (Utah 2004).

129. Missouri is considering—for the third time—a bill targeted at EPC-tagged consumer products, but that bill is currently in the same committee that killed the two earlier attempts. *See* S.B. 638, 93d Gen. Assem., 2d Reg. Sess. (Mo. 2006). After more than a year of inactivity, a bill in the Tennessee House was assigned to subcommittee and then promptly removed from the subcommittee's calendar. *See* H.B. 300, 104th Gen. Assem., Reg. Sess. (Tenn. 2005). The Massachusetts House and Senate are considering identical bills targeted at EPC-tagged consumer products. *See* H.B. 1447, 184th Gen. Ct., Reg. Sess. (Mass. 2005); S.B. 181, 184th Gen. Ct., Reg. Sess. (Mass. 2005). Both bills were referred to committee in January 2005. A source in State Senator Jarrett T. Barrios's office advised that the Senate version's reporting date was extended until June 15, 2006, and that Senator Barrios planned to argue that the bill should be presented to the full Senate for a vote. However, on May 30, 2006, the Senate sent the bill packing to a "joint committee . . . to make an investigation and study of" the issues addressed in the bill—which may be its death knell. S2564-SJ 2081, Order History, http://www.mass.gov/legis/184history/s02564.htm (last visited Dec. 22, 2006); *see also* S.B. 181, Bill History, http://www.mass.gov/legis/184history/ s00181.htm (last visited Dec. 22, 2006). The bill in the House is suffering an identical fate. *See* H. 5007, Order History, http://www.mass.gov/legis/184history/h05007.htm (last visited Dec. 22, 2006); *see also* H.B. 1447, Bill History, http://www.mass.gov/legis/184history/h01447.htm (last visited Dec. 22, 2006).

130. *See* H.B. 354, 419th Gen. Assem., Reg. Sess. (Md. 2005); *see also* H.B. 32, 418th Gen. Assem., Reg. Sess. (Md. 2004); H.B. 1304, 2004 Gen. Assem., Reg. Sess. (Va. 2004); S.J.R. 10, 55th Leg., Gen. Sess. (Utah 2004).

131. H.B. 1114, 80th Legis. Assem., Reg. Sess. (S.D. 2005).

132. *See* H.B. 1114, Bill Action Summary, http://legis.state.sd.us/sessions/2005/1114.htm (last visited Dec. 22, 2006).

have had any potential effect on the future of contactless payment systems.

In the midst of all the carnage from bills killed in other states, New Hampshire considered a bill to prohibit the state's participation in a national identification card system under the Real ID Act[133] and enacted a bill prohibiting the use of radio frequency devices to identify the occupants of motor vehicles while on any public road or street in the state.[134] The bill opposing national identification cards, however, met a fate identical to the original version of House Bill 203-FN, which sought to impose comprehensive requirements on the use of RFID technology in New Hampshire.[135] House Bill 203-FN passed the New Hampshire

133. *See* Introduction of H.B. 1582, 159th Gen. Ct., 28 H. Rec. No. 7, H.J. No. 1, Jan. 4, 2006, *available at* http://gencourt.state.nh.us/hcaljourns/journals/2006/houjou2006_7.html. After passing in the House, the New Hampshire Senate amended H.B. 1582 into an Act to merely "establish a commission to study the Real ID Act of 2005." H.B. 1582, 159th Gen. Ct., Reg. Sess. (N.H. 2006), *available at* http:/www.gencourt.state.nh.us/legislation/2006/HB1582.html. It appears even the stripped-down version has been killed in the Senate. *See* H.B. 1582 Activity & Status, http://www.generalcourt.org/bills/2006/HB1582/ status (last visited Dec. 22, 2006).

134. H.B. 1738-FN, 159th Gen. Ct., Reg. Sess. (N.H. 2006), *available at* http://www.gencourt.state.nh.us /legislation/2006/HB1738.html.

135. H.B. 203-FN, 159th Gen. Ct., Reg. Sess. (N.H. 2006) (showing the bill's text as amended and passed by the New Hampshire House). The version of the bill passed by the New Hampshire House is no longer available on the New Hampshire General Court's bill tracking system. The bill, as amended by the New Hampshire House, addressed any RFID tag capable of transmitting individuals' nonpublic personal information, including "name, address, [phone numbers], social security number, credit card and financial account numbers, driver's license number, e-mail address, date of birth, race, religion, ethnicity, nationality, political affiliation, photograph and digital image, fingerprint or other biometric identification, and any other unique personal identifier or number." *Id.* This description encompassed contactless payment systems, but only required that credit, debit, or other financial account cards containing RFID-enabled microchips bear a label containing a "universally accepted symbol" to designate the RFID transponder's presence, frequency, and data structure. *Id.* The bill would also have prohibited the implantation of subdermal RFID devices in individuals "without the informed, written consent of the individual, or an individual's legal guardian," and would have prohibited offering incentives, denying opportunities, or "in any way treat[ing any individual] differently from any other individual as a consequence of providing or withholding such consent." *Id.* State Representative Howard C. Dickinson, the bill's primary sponsor, never responded to the author's inquiry about the changes to the original House version of the bill.

Considering that much less restrictive measures in other states had already failed, it seemed doubtful that New Hampshire's bill would succeed. Even if the bill had become law, a label on each contactless payment device designating the RFID transponder's presence, frequency, and data structure would not have addressed the privacy concerns caused by contactless payment systems. It appeared New Hampshire would have been satisfied as long as a label was present to make customers aware of the presence of RFID-enabled microchips in their contactless payment devices.

House, but after a hearing in the Senate on March 8, 2006, the bill was renamed and amended to merely "establish[] a commission . . . [to] study the use of radio frequency technology in the private and public sectors, its benefits, and potential privacy implications."[136] Given the far-flung failures of privacy-related RFID technology bills and the fact that the final versions of both House Bills 203-FN and 1582 were stripped of their original teeth, it seems unlikely that New Hampshire will enact any legislation restricting RFID technology.

2. Congress Only Mulls Privacy Legislation Aimed at EPC-Tagged Consumer Products

In mid-2003, the non-profit organization Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN) unveiled its model RFID Right to Know Act of 2003, "calling for mandatory disclosures on *consumer products* containing [EPC tags]" in order to "protect consumers against unwittingly purchasing products embedded with remote surveillance devices."[137] Despite including "ATM cards" in the list of things people buy that could be embedded with RFID-enabled microchips,[138] CASPIAN did not articulate a specific need for privacy legislation regarding contactless payment systems, and even if it had, the Act's narrow purpose was merely "[t]o require that commodities containing radio frequency identification tags bear labels stating that fact."[139]

In 2004, the federal government responded with equally narrow vision. At a Federal Trade Commission (FTC) workshop entitled Radio Frequency Identification: Applications and Implications for Consumers, Beth Givens of the PRC explained that RFID "could threaten privacy and civil liberties" and "call[ed] for a comprehensive multi-disciplinary 'technology assessment' of RFID."[140] However,

136. H.B. 203-FN, 159th Gen. Ct., Reg. Sess. (N.H. 2006), *available at* http://www.gencourt.state.nh.us/legislation/2006/HB0203.html (showing the bill's title and text as amended and passed by the New Hampshire Senate).

137. Press Release, CASPIAN, Consumer Group Unveils RFID Labeling Legislation (June 11, 2003), *available at* http://www.spychips.com/press-releases/right-to-know-release.html (emphasis added).

138. *Id.*

139. *See* Summary of RFID Right to Know Act, http://www.spychips.com/press-releases/right-to-know-summary.html (last visited Dec. 22, 2006) (including the full text of the proposed legislation).

140. Beth Givens, Dir., PRC, Presentation at the Federal Trade Commission RFID Workshop, Implementing RFID Responsibly: Calling for a Technology Assessment (June 21, 2004), http://www.privacyrights.org/ar/FTC-RFIDTestimony.htm (emphasis added).

Givens only discussed RFID technology in the context of EPC tags as UPC bar code replacements, again failing to address privacy concerns caused by either contactless payment systems or other RFID applications.

Two days after the FTC workshop, Representative Gerald Kleczka proposed the Opt Out of ID Chips Act,[141] a bill significant for two reasons: (1) it only addressed privacy concerns with EPC tags as UPC bar code replacements, and (2) it marked the first—and last—time Congress addressed RFID's impact on individuals' privacy rights. The Act would have made it a deceptive or unfair practice for a retailer to sell a product containing an EPC tag unless: (1) the product bears a label stating it contains an EPC tag, (2) the label notifies the customer that he or she has the right to have the EPC tag removed or disabled at the point-of-sale, and (3) the customer is actually given the option of removing or disabling the EPC tag at the point-of-sale. Shortly after the bill's referral to the House Energy and Commerce Committee, the Subcommittee on Commerce, Trade, and Consumer Protection held a hearing entitled *Radio Frequency Identification (RFID) Technology: What the Future Holds for Commerce, Security, and the Consumer*.[142] Representative Cliff Stearns, subcommittee chairperson, opened with remarks indicating the hearing was supposed to have a broad purpose:

> I'm pleased to say that this subcommittee will attempt to get out in front and conduct the first congressional hearing on . . . [RFID] technology . . . .
>
> . . . .
>
> . . . [O]ur job [is] to cut through [the] hype, get the facts about RFID, learn more about its applications, and examine the public policy issues generated by its use and widespread deployment.[143]

Despite Representative Stearns's intention to "get out in front" of RFID technology, his comments seemed to foreshadow a narrow focus on EPC-tagged consumer products:

> These RFID tags can be attached to products and packaging individually.
>
> . . . .

141. H.R. 4673, 108th Cong. (2d Sess. 2004).

142. *Hearing*, *supra* note 8.

143. *Id.* at 1, 3 (statement of Hon. Cliff Stearns, Chairman, Subcomm. on Commerce, Trade, and Consumer Protection). Note that Representative Stearns referred to RFID's "applications" in the plural, hinting that the discussion to come would cover the details of at least several RFID applications. *Id.*

> . . . [W]ork is being done to develop common standards known as the Electronic Products Code or "EPC" . . . . [which] would allow RFID readers to receive EPC data from tags on items and products . . . .
>
> . . . [T]his is a global effort and, in theory, could lead to a seamless supply chain and logistics management in global trade.[144]

Representative Stearns alluded once to contactless payment systems:

> One possible future application . . . involves using readers at checkout. . . . [to] allow customers to pass straight through with their RFID tagged items loaded in their shopping carts. Customer accounts would be automatically updated leaving them free to head straight for the parking lot.[145]

However, neither Representative Stearns nor any other member recognized the privacy concerns caused by "automatic" payment technology.

Representative Janice Schakowsky voiced the strongest criticisms of RFID technology in her opening comments, but also seemed to join the chorus focusing only on concerns with EPC tags embedded in such objects as clothing and passports.[146] Representative Schakowsky indicated that she saw no privacy concerns with contactless payment systems, stating that she appreciated the convenience RFID technology brought to "E-Z passe [sic] and SmartCards for public transportation."[147]

It is possible that the hearing's narrow focus was inevitable. Dr. Sanjay Sarma of the Massachusetts Institute of Technology, the first presenter to speak at the hearing, stated that his comments were "focused entirely on the supply chain, because that is where the interest primarily now lies and what the current technology is capable of providing."[148] Sarma's gauge for assessing those interests appears to have been drawn from his projection that replacing UPC bar codes with EPC tags could generate savings in excess of $550 billion per year.[149]

144. *Id.* at 1–2.

145. *Id.* at 2.

146. *Id.* at 3 (statement of Hon. Janice Schakowsky, Member, Subcomm. on Commerce, Trade, and Consumer Protection).

147. *Id.* at 4.

148. *Id.* at 13 (prepared statement of Sanjay Sarma, Assoc. Professor, Mass. Inst. Tech.).

149. Accenture, a management consulting and technology services company, estimated that "RFID could eliminate 15 to 30 percent of missing inventory," that "the retail industry alone loses more than $50 billion a year to theft, paperwork errors, and vendor fraud," and

But it was Sarma's assertion that EPC tags as UPC bar code replacements represented the full expression of "what the current technology [was] capable of providing," coupled with his assertion that it was "impossible to anticipate the full spectrum of uses to which RFID [t]echnology . . . will be placed" that may have discouraged any in-depth discussion of any other RFID application.[150]

Sarma's intention to focus the hearing on EPC tags surfaced in his very first sentence. To explain how RFID-enabled microchips work, Sarma held up two EPC tags and said, "An RFID tag is a chip and an antenna. It has no battery. It is simply a chip and an antenna."[151] By this, Sarma made it clear that he would address only passive RFID technology as active RFID microchips contain batteries;[152] he thus ignored the VeriChip and contactless payment systems that operate on NFC technology. Next, Sarma demonstrated that his sample EPC tag had a read range of about ten feet[153] but did not mention that the read range of any RFID tag, whether operating on a low or high frequency, is as much dependent on the power and size of the reader's antenna. Sarma did not demonstrate how a high-power antenna could be used to increase the read range of any RFID tag.[154] No subcommittee member or privacy advocate present at the hearing questioned or challenged Sarma's omissions. Following the demonstration, Sarma continued his narrow focus, opining that "where [RFID is] heading" is only to "lubricate the supply chain" from manufacturer to retailer and to produce "better shopping experiences for consumers and [improved]

that "[p]roduct counterfeiting costs another $500 billion a year worldwide." *Id.* Researchers at Emory University concluded that "the average retailer loses 4 percent of its sales due to out-of-stock" items. *Id.* at 17 (prepared statement of Linda M. Dillman, Exec. Vice President & Chief Info. Officer, Wal-Mart Stores, Inc.). Wal-Mart reported $312.4 billion in sales in the fiscal year ending January 31, 2006. *See* Wal-Mart, Corporate Facts: Wal-Mart By the Numbers, http://www.walmartfacts.com/FactSheets/10242006_Corporate_Facts.pdf (last visited Dec. 22, 2006). If Wal-Mart lost four percent of its annual sales due to out-of-stock items, it would lose $12.5 billion in sales per year. In other words, Wal-Mart's annual lost sales due to out-of-stock items alone could equal the 2004 gross national income of Estonia, the world's 98th largest economy. *See* WORLD BANK, WORLD DEVELOPMENT INDICATORS DATABASE (2006), http://siteresources.worldbank.org/DATASTATISTICS/Resources/GNI.pdf.

150. *Hearing*, *supra* note 8, at 13 (prepared statement of Sanjay Sarma, Assoc. Professor, Mass. Inst. Tech.).

151. *Id.* at 7.

152. Passive RFID chips do not have a battery; active RFID chips have batteries. That's what makes them "active." *See supra* note 40 and accompanying text.

153. *Hearing, supra* note 8, at 8 (statement of Sanjay Sarma, Assoc. Professor, Mass. Inst. Tech.).

154. *See supra* note 67 and accompanying text.

efficiency all across the global supply chain."[155] It was clear that Sarma would not acknowledge privacy concerns caused by contactless payment systems or any other RFID application.

Sarma's presentation also provided support for RFID proponents' assertions that privacy concerns about RFID are overblown and that legislators should permit self-regulation. Sarma's proposed guidelines for companies engaged in the "large-scale deployment of EPC" to use in developing their own privacy practices only addressed EPC tags as UPC bar code replacements: (1) give consumers notice of EPC tags on product packaging, (2) give consumers the option to disable or remove EPC tags on products purchased, (3) make it easy for consumers to get information on EPC tags, and (4) require companies using data generated through EPC to comply with applicable laws.[156]

Ultimately, the subcommittee went no further than where Sarma and the other testifying RFID proponents led it. Linda Dillman, Chief Information Officer for Wal-Mart, asserted that "[i]n the future, EPCs have the potential to help us minimize wait time at checkouts," but that "[t]here is no additional information about individuals, available or collected, via RFID because [EPC] codes identify products and not people."[157] Even though Dillman did not acknowledge the potential impact on individuals' privacy rights of any RFID application other than EPC tags, Dillman's assurances that Wal-Mart would not collect data from RFID tags in any form is contradicted by Wal-Mart's own consumer privacy policy, a copy of which Dillman provided in her prepared statement. The policy states that Wal-Mart "will collect and use . . . information about you which is, or can be, tied to you as an individual" including "identification numbers, account numbers, product preferences, and other information you provide when you do business with us . . . [and] financial . . . information provided by you . . . in connection with your transactions."[158] It is noteworthy that within months of the hearing, Wal-Mart introduced a Wal-Mart Credit Card and a Wal-Mart Discover Card[159]—cards that could easily be

155. *Hearing, supra* note 8, at 9–11 (prepared statement of Sanjay Sarma, Assoc. Professor, Mass. Inst. Tech.).

156. *Id.* at 12.

157. *Id.* at 14 (statement of Linda M. Dillman, Exec. Vice President & Chief Info. Officer, Wal-Mart Stores, Inc.).

158. *Id.* at 18–19.

159. Wal-Mart's two new credit cards were introduced on February 22, 2005. David Wells, *Morgan Stanley Faces Investor Grilling Over Discover Card Unit*, FIN. TIMES, Mar. 10, 2005, at 29.

issued in contactless payment device form factors in the near future. GE Money Bank (GEMB), the issuer of the two cards, states that it will provide Wal-Mart and its affiliates, licensees, and "third-party service providers (such as modeling and database companies)" with cardholders' nonpublic personal information on a scale much greater and more invasive than Wal-Mart's own privacy policy: GEMB can provide Wal-Mart with cardholders' transaction information on the Wal-Mart Discover Card even when cardholders' transactions are not made at Wal-Mart.[160]

While Sarma and Dillman narrowed the subcommittee's focus, William Galione of Philips Semiconductors expressly dismissed the possibility that contactless payment systems could cause privacy concerns. Galione admitted that one of the "most common applications of contactless identification technology" is its use "by people to identify themselves," including, for example, using "'[s]mart cards' [that] typically come in a credit card form factor and carry sensitive, personally identifiable data."[161] However, Galione dismissed privacy concerns about any type of contactless identification device as unwarranted because such contactless devices are readable from only "three to four inches away," are "very, very secure . . . [with] advanced encryption technologies[,] . . . password protection and mutual authentication between the card and the reader,"[162] and offer the "enhanced security and privacy protection" of "biometric credentials."[163]

160. *See* Wal-Mart Credit Services, http://www.walmartcreditcard.com (last visited Dec. 22, 2006). Wal-Mart's credit cards are issued through GE Money Bank (GEMB), a member of the General Electric corporate family. *Id.* GEMB's privacy policy promises that "through your use of [the Wal-Mart credit cards]" GEMB will "collect personally identifiable information about you . . . [including] transaction information about items purchased . . . for identification . . . servicing and marketing purposes." *See* Wal-Mart Financial Services, Wal-Mart Credit Card and Wal-Mart Discover GE Money Bank Privacy Policy, https://www.onlinecreditcenter2.com/walmartstorecard/csgen2w2/WFWprivacy.htm (last visited Dec. 22, 2006). Upon collecting this information, GEMB promises to share it with, amongst others, "Wal-Mart Stores, Inc. and its affiliates . . . licensees, or third-party service providers (such as modeling and database companies)" for any purpose "permitted by law." *Id.*

161. *Hearing, supra* note 8, at 32–33 (prepared statement of William Galione, Vice President & Gen. Manager, Philips Semiconductors).

162. *Id.* at 30–31 (statement of William Galione, Vice President & Gen. Manager, Philips Semiconductors).

163. *Id.* at 33 (prepared statement of William Galione, Vice President & Gen. Manager, Philips Semiconductors). As proof, Galione offered: "The DoD makes worst case scenario assumptions about [its contactless identification] cards falling into the wrong hands and having large resources at their disposal to crack the card—standards that advanced smart cards have met through the use of encryption, secure design, and other measures." *Id.*

Galione ultimately addressed privacy solely in the context of EPC-tagged consumer products.[164] No subcommittee member or privacy advocate in attendance challenged Galione's summary dismissal of privacy concerns caused by contactless payment systems.

Each privacy advocate who testified focused almost exclusively on EPC-tagged consumer products. Paula Bruening of the Center for Democracy and Technology (CDT) identified as one of the "novel privacy issues raised by RFID" the reality that "[d]iscount cards, other 'customer loyalty cards' and credit cards already collect information about individuals, providing a rich store of information about our likes and dislikes."[165] However, Bruening turned her focus to EPC-tagged consumer products,[166] perhaps due to a perception that any privacy issues caused by contactless payment systems would be addressed by federal privacy laws already regulating "credit cards . . . and financial records."[167] One of Bruening's greatest concerns was that data from EPC-tagged consumer products would be collected without the "active engagement" of consumers.[168] Bruening explained by using a credit card transaction analogy:

> When I used [sic] a credit card, I am actively deciding to turn over certain information that will make it possible to complete a transaction. . . . RFID data collection . . . . does not actively engage the consumer at all and provides the consumer with no record that the data collection ever happened.[169]

Arguably, a person using a contactless payment device to make a payment transaction may not have a legitimate expectation of privacy at that moment since he or she, just like a person using a credit or debit card, would be voluntarily disclosing the data necessary to make a payment transaction.[170] However, this reasoning ignores the major

164. *Id.*

165. *Id.* at 26 (prepared statement of Paula J. Bruening, Staff Counsel, CDT).

166. *Id.* at 24 (statement of Paula J. Bruening, Staff Counsel, CDT). Some of Bruening's greatest concerns were that EPC tags "[i]nserted into the sleeve of a blouse or the hem of a pair of trousers" would permit an "invisible," "more fine grained [method of] data collection than previously possible," that consumers may not know such EPC tags were present, and that the information collected about the consumer would be without the consumer's "active engagement." *Id.*

167. *Id.* at 27 (prepared statement of Paula J. Bruening, Staff Counsel, CDT). Bruening may have been referring to the Gramm-Leach-Bliley Act (GLBA). *See infra* notes 189–191 and accompanying text.

168. *Hearing, supra* note 8, at 24 (statement of Paula J. Bruening, Staff Counsel, CDT).

169. *Id.*

170. *Id.* Bruening's logic is similar to that applied in *Katz v. United States* where the Court stated individuals do not have a legitimate expectation of privacy in things they

difference between credit and debit cards and contactless payment devices: traditional credit and debit cards with magnetic stripes can only be read when swiped through a POS terminal during a payment transaction or by other devices capable of reading magnetic stripes, while contactless payment devices can be read from a distance even when individuals are not using their devices to make payments.

In other testimony at the hearing, Cédric Laurant of the Electronic Privacy Information Center (EPIC) mentioned, in passing, "electronic roadway toll collection,"[171] but then focused his attention solely on the use of EPC tags as UPC bar code replacements.[172] Barry Steinhardt of the ACLU addressed "consumer issues"[173] that dealt only with "retailers . . . engaged in a major push to advance adoption of RFID technology . . . [with] RFIDs eventually replacing UPC bar codes on products."[174] Steinhardt provided several scenarios to illustrate his concerns, but each dealt only with the ability to track and profile individuals using EPC tags in consumer goods.[175]

Ultimately, the broad reaches of RFID technology on commerce, security, and consumers were not discussed; the hearing, instead, focused almost exclusively on EPC tags as UPC bar code replacements. Representative Kleczka's bill never made it past the subcommittee, and no RFID privacy legislation has since been introduced. Privacy concerns about RFID applications appear to be dead at both the state and federal levels without any meaningful discussion of the privacy concerns caused by contactless payment systems.

III. IN SEARCH OF AN APPROPRIATE PUBLIC POLICY RESPONSE

A. Privacy Advocates Rely on Inapposite Fair Information Principles

Privacy advocates' proposals for regulating RFID technology do not address privacy problems caused by contactless payment systems. In his

"knowingly expose[] to the public." Katz v. United States, 389 U.S. 347, 351 (1967). While this logic may form the test for individuals' constitutionally-protected privacy interests, it should not be the basis for determining whether privacy legislation directed at contactless payment systems is warranted.

171. *Hearing*, *supra* note 8, at 44 (statement of Cédric Laurant, Policy Counsel, EPIC).

172. *See generally id.* at 35–39 (prepared statement of Barry Steinhardt, Dir. of the Tech. and Liberty Program, ACLU).

173. *Id*. at 38 (discussing "proposals to incorporate RFID tags into government identity documents").

174. *Id*.

175. *See generally id*. at 34–39.

hearing testimony, Cédric Laurant advocated RFID-specific legislation to protect individuals' privacy for "all forms of RFID-based services"[176] but did not articulate specific details on how he would address RFID applications other than EPC tags as UPC bar code replacements. In contrast, Paula Bruening urged Congress not to enact legislation affecting any RFID application for fear of "technology mandates" that would be "ill-suited to the future evolution of the technology,"[177] and called instead for "baseline privacy legislation" based on "principles of fair information practices."[178] The "common elements" of these principles suggest that collection of individuals' personal data "should be open and transparent," that personal data collected "should be relevant to . . . [and] used only for the purpose for which it was collected," that it "should be accurate, complete, and timely," that it "should be protected by reasonable security safeguards," that "[i]ndividuals should have a right to view . . . [and] correct" data collected about them, and that entities maintaining such data "should be accountable for complying with fair information practices."[179]

While Bruening asserted that these principles "provide a starting point for all ongoing and future efforts to understand and address the RFID privacy issue,"[180] Laurant, who had supported Bruening's position on the fair information principles at the subcommittee hearing, later called a set of self-regulatory guidelines developed from the same principles "inadequate" because "they failed to give consumers adequate privacy protection."[181] First, Laurant asserted that these principles were inadequate "because they fail[ed] to provide an enforcement mechanism" for individuals if and when an entity violated one of the principles.[182] Second, the principles made "'suggestions, but

176. *Id.* at 48 (statement of Cédric Laurant, Policy Counsel, EPIC). Laurant advocated that the legal framework for RFID privacy legislation could be the same fair information principles Bruening discussed. *Id.* at 44.

177. *Id.* at 26, 29 (statement of Paula J. Bruening, Staff Counsel, CDT).

178. *Id.* at 26.

179. *Id.* at 27.

180. *Id.*

181. *RFID: International Chamber of Commerce Issues Privacy Protection Guidelines on Use of RFID*, Privacy L. Watch (BNA), at D-11 (Apr. 25, 2005). Laurant criticized the International Chamber of Commerce's "guidelines designed to quiet privacy concerns surrounding the use of Radio Frequency Identification systems, urging businesses to engage in self-regulation as a way of earning consumer confidence and preventing the emergence of conflicting RFID laws and regulations around the globe," even though the guidelines appeared to be a near point-for-point adoption of the fair information principles Laurant had earlier supported. *Id.*

182. *Id.*

[did not] require anything.'"[183] Third, the principles did not "mak[e] sure that consumers provide informed and unambiguous consent before their information is collected and used."[184]

In addition to the shortcomings Laurant articulated, there are other reasons the fair information principles are not sufficient to address privacy concerns caused by contactless payment systems. An individual's ability to voluntarily choose his or her method of payment for any transaction, including anonymous cash transactions, must be guaranteed, but these principles do not recommend such voluntary participation. Further, information collected and used in connection with these principles is not truly "fair" if an individual's "choice" to use contactless payment devices is not always voluntary. Finally, these principles incorrectly assume that all entities or persons who interrogate contactless payment devices to collect the stored information will act in accordance with the values of openness, transparency, relevance, reasonableness, and accountability.

The European Commission, generally regarded by privacy advocates as far ahead of the United States in protecting individuals' privacy rights, set up an Article 29 advisory group to "look into the privacy and other fundamental rights implications of RFID technology."[185] The advisory group cited as its impetus the fact that "RFID technology is taking off in a variety of sectors," including "Retail Applications."[186] However, the working group's only acknowledgment of retail or retail-related applications is the planned adoption of EPC tags to replace UPC bar codes.[187] Nowhere did the advisory group identify or discuss the possibility that privacy problems could be caused in the financial services sector through the widespread distribution and use of contactless payment devices, and the data security principles articulated by the advisory group[188] appear to have been echoed in the fair information principles espoused by privacy advocates in the United States.

183. *Id.*

184. *Id.*

185. Article 29 Data Protection Working Party, *Working Document on Data Protection Issues Related to RFID Technology*, 10107/05/EN WP 105, at 2 (Jan. 19, 2005), *available at* http://www.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf.

186. *Id.* at 3–5.

187. *Id.* at 4, 13.

188. *See generally id.*

B. Contactless Payment Proponents Hide Behind the Gramm-Leach-Bliley Act and Self-Regulation Proposals

Title V of the Gramm-Leach-Bliley Act (GLBA)[189] deals with privacy issues and requires, inter alia, the

> clear disclosure by all financial institutions of their privacy policy regarding the sharing of non-public personal information with both affiliates and third parties[,] . . . a notice to consumers and an opportunity to "opt-out" of sharing of non-public personal information with nonaffiliated third parties subject to certain limited exceptions[, and] . . . the disclosure of a financial institution's privacy policy . . . at the time of establishing a customer relationship with a consumer and not less than annually during the continuation of such relationship.[190]

However, the GLBA provides no meaningful protection for the nonpublic personal information of the customers of financial institutions, making the GLBA woefully inadequate to address privacy concerns caused by contactless payment systems.

First, the GLBA applies only to financial institutions that collect and disclose their customers' personal financial information and to any company that receives such information from a financial institution.[191] Thus, entities or persons who are not financial institutions and who collect and disclose either financial or non-financial personal information obtained from consumers' contactless payment devices or payment transactions are not required to comply with the GLBA. For example, GEMB issues the Wal-Mart Credit Card and Wal-Mart Discover Card, is a financial institution governed by the GLBA, and thus must comply with the GLBA. In contrast, Wal-Mart—not likely a "financial institution"—could begin accepting contactless payment transactions, then collect, store, and share the nonpublic personal data it obtained by interrogating the contactless payment devices of both GEMB account holders and all other customers carrying other contactless payment devices such as Chase's blink card or MasterCard's PayPass. Since Wal-Mart would not likely be considered a financial institution under the GLBA, it appears Wal-Mart could collect and disclose both financial and non-financial information obtained from all

189. Gramm-Leach-Bliley Financial Services Modernization Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified at 15 U.S.C. §§ 6801–6809 (2000)).

190. CRA Amendments in the Gramm-Leach-Bliley Act, Summary of Provisions, http://banking.senate.gov/conf/grmleach.htm (last visited Dec. 22, 2006).

191. *See* Privacy Initiatives, The Gramm-Leach-Bliley Act: The Financial Privacy Rule, http://www.ftc.gov/privacy/privacyinitiatives/financial_rule.html (last visited Dec. 22, 2006).

its customers' contactless payment devices or payment transactions with no requirement to comply with the GLBA.

Second, the GLBA does not regulate how financial institutions protect individuals' privacy—it only requires that financial institutions disclose their privacy policies to their customers and allow customers to request that their nonpublic personal information not be shared with other companies. This means each financial institution issuing contactless payment devices is free to decide how and to what extent it will protect its customers' privacy, if at all, and is free to share the nonpublic personal information of any customers who have not opted-out of the financial institution's information sharing scheme with other, even non-affiliated, companies.

Finally, since the GLBA leaves it up to financial institutions to establish their own privacy policies, there is no mandate that financial institutions permit voluntary participation—for example, financial institutions can require consumers to accept a contactless payment device in order to obtain an account. There is, additionally, no requirement that financial institutions obtain their customers' affirmative opt-in to financial institutions' information sharing schemes, no minimum required encryption or other data security standards, and no limit to the purposes for which financial institutions may interrogate their customers' contactless payment devices, especially when customers are not in the process of making payment transactions. There is also no prohibition against a financial institution interrogating the contactless payment devices of any non-customer consumers for any purpose.

Despite the GLBA's shortcomings, many companies, including those currently issuing contactless payment devices to their customers, have implemented privacy policies that appear tailored to meet the GLBA's requirements, perhaps as a preemptive move in hopes of avoiding additional privacy legislation.[192] Among contactless payment device issuers, ExxonMobil appears to have strictly followed the GLBA's requirements in its Speedpass privacy policy,[193] whereas MasterCard, Visa, and Chase merely apply the privacy policies for their regular credit and debit card products to their contactless payment programs—privacy policies governed specifically by the GLBA.[194]

192. *See* notes 157–160 and accompanying text.

193. *See* Speedpass Consumer Privacy Policy, https://www.speedpass.com/forms/frmPrivacy2.aspx (last visited Dec. 22, 2006).

194. Chase does not have a privacy policy tailored specifically to its blink card. *See generally* Chase Privacy Policy, http://www.chase.com/ccp/index.jsp?pg_name=ccpmapp/

Applied Digital has articulated privacy guidelines for its VeriChip that are markedly different from the GLBA's requirements, but Applied Digital has not obligated itself to very much: VeriChip subscribers' participation "*should* be voluntary[,] . . . subscribers *are* able to have their VeriChip removed and discontinued at any time," and only subscribers *should* choose who has access to their nonpublic personal information stored in Applied Digital's databases.[195] Otherwise, Applied Digital offers that its Chief Privacy Officer will stay on top of "the day-to-day global evolution of" RFID technology, "immediately address" subscribers' privacy concerns, and "engage government, privacy groups, the industry and consumers to assure that the adoption of VeriChip and RFID technology is through education and unity rather than isolation and division."[196]

Among Applied Digital's guidelines, voluntary participation and discontinuance are most critical to contactless payment systems. If individuals are ever *required* to use contactless payment devices to do business with any bank or merchant, such a condition would eliminate the anonymity currently afforded to individuals by virtue of the ability to make cash transactions.[197] In discussing voluntariness, however, it is noteworthy that Applied Digital used words like "should" and "are" rather than "must" and "shall," indicating it may be all too willing to cooperate if the federal government ever requires mandatory chipping of individuals for secure identification or other purposes.

Problems with Applied Digital's other suggestions prevent its guidelines from being effective for contactless payment systems. First, Applied Digital's commitment to have its Chief Privacy Officer stay abreast of RFID technology does not guarantee its subscribers' privacy.

shared/assets/page/Privacy_Policy (last visited Dec. 22, 2006). MasterCard does not have a privacy policy tailored specifically to its PayPass card. *See* MasterCard PayPass, http://www.mastercard.com/us/personal/en/aboutourcards/paypass/index.html (last visited Dec. 22, 2006) ("Current MasterCard and Issuer privacy and confidentiality rules apply as per your current cardholder agreement."). Visa does not have a privacy policy tailored specifically to its Visa Contactless card. *See* Visa USA, Personal: Visa Contactless, http://www.usa.visa.com/personal/cards/contactless/ (last visited Dec. 22, 2006) ("Visa Contactless provides you with the same security protection you get with the traditional Visa cards, including Zero Liability.").

195. Press Release, VeriChip, Applied Digital Announces Six Point Privacy Statement at ID World Congress in Barcelona, Spain (Nov. 22, 2004), *available at* http://www.verichipcorp.com/news/1101103200.

196. *Id.*

197. This assumes, of course, that RFID tags are not embedded in currency, an idea already considered by the European Union. Kim Yong-Young, *Radio ID Chips May Track Banknotes*, CNET NEWS.COM, May 22, 2003, http://news.com.com/2100-1017-1009155.html.

Second, Applied Digital's commitment to immediately address subscribers' privacy rights in documents related to VeriChip only obligates Applied Digital to respond to privacy concerns raised by its subscribers—it does not obligate Applied Digital to protect its subscribers' privacy proactively. Third, allowing subscribers to have their VeriChip removed at any time reinforces Applied Digital's commitment to voluntary participation, but it does not strengthen privacy protections. For example, security breaches that result in the theft of its subscribers' nonpublic personal information may be the very reason subscribers choose to have their VeriChip removed. Fourth, allowing customers to designate who can access their nonpublic personal information could exponentially increase the number of attack points from which Applied Digital's databases could be compromised, thus harming rather than protecting its subscribers' privacy. Finally, a notable omission: Applied Digital made no commitment to develop a means of preventing the VeriChip from responding to unauthorized RFID readers. Without such a security feature, which may not be technologically or economically feasible, a VeriChip used as a contactless payment device could be susceptible to tracking much like any consumer product containing an EPC tag.

Others have discouraged RFID privacy legislation in the name of advancing technology. In his hearing testimony, Sarma pressed Congress to forego RFID privacy legislation in order to realize "the many benefits associated with this exciting technology."[198] Sarma asserted that a hands-off approach would be appropriate since the EPCglobal Network[199] had already "adopted guidelines for use by all companies engaged in the large-scale deployment of EPC" and that "[t]hese guidelines [were] intended to complement the national . . . laws and regulations dealing with consumer protection, consumer privacy,

198. *Hearing*, *supra* note 8, at 13 (prepared statement of Sanjay Sarma, Assoc. Professor, Mass. Inst. Tech.).

199. *See id.*

> In 1999, the Uniform Code Council, Inc. . . . joined with Procter & Gamble and The Gillette Co. in helping establish the Auto-ID (Automatic Identification) Center at the Massachusetts Institute of Technology (MIT). . . . The center's mission was to develop RFID for use across the global supply chain.
>
> . . . .
>
> By November, 2003, enough progress had been made in these efforts to create . . . EPCglobal Inc., with the mission of developing the technical standards pertaining to [the network in which EPC tags could be used] and driving their adoption across industries and across the world.

Id. at 11.

and related issues."[200] Sarma promised that consumers would be given clear notice of products bearing EPC tags, would be allowed to disable or remove EPC tags from products they purchased, and would get to learn about RFID technology and its benefits while having time to get comfortable with an EPC logo indicating the presence of an RFID tag, and that "[c]ompanies [would] use, maintain, and protect records generated through EPC in compliance with all applicable laws."[201]

None of these guidelines address the privacy concerns caused by contactless payment systems. First, even if individuals are given clear notice of the presence of a contactless smart chip in their contactless payment devices, the only choice individuals have, assuming their contactless payment devices are in form factors other than traditional credit or debit card plastics, is to return the contactless payment device. Individuals would not be able to discard, disable, or remove the contactless smart chip and still have a functioning contactless payment device. Second, allowing individuals to learn about the technology behind their contactless payment device does nothing to protect individuals' privacy; likewise, merely emblazoning a logo on contactless payment devices to allow users to get comfortable with an RFID-enabled microchip's presence does nothing to protect individuals' privacy. In fact, providing lessons on RFID and placing logos on devices may do nothing more than raise questions in individuals' minds about just how much privacy they ceded by deciding to accept and use contactless payment devices. Finally, even though banks and merchants may agree to protect records generated through the use of contactless payment systems, such a commitment does not eliminate security-related privacy concerns[202] and does not address the potential for individuals to be profiled or tracked by their contactless payment devices since no laws prohibiting such activity exist.

C. A Bill to Protect Individual Privacy Without Stifling Technology

The privacy problems caused by contactless payment systems should be addressed now to establish appropriate boundaries for RFID technology rather than allowing the boundaries to be set, by default, at the outer limits of the technology's full capacity. While not intended to

200. *Id.* at 12. It is unclear to which laws Sarma was referring since no privacy laws directed at RFID have been enacted. If Sarma was referring, in part, to the GLBA, this was a hollow promise. *See supra* notes 189–194.

201. *Hearing*, *supra* note 8, at 12.

202. *See supra* notes 65–95 and accompanying text.

be an exhaustive list, the following principles establish a starting point to achieve two critical legislative goals: (1) give every individual as much control as is practicably possible over access to his or her nonpublic personal information, and (2) avoid impeding the development of contactless payment system technology.

Accordingly, lawmakers should incorporate the following principles in legislation addressing the privacy problems caused by contactless payment systems:

(1) All contactless payment devices manufactured for distribution in the United States shall include a minimum of 128-bit and triple DES encryption;

(2) All persons who issue contactless payment devices to their customers shall encrypt all data stored on or transmitted by such contactless payment devices, including each device's EPC;

(3) All contactless payment devices manufactured for distribution in the United States shall be capable of interrogation or data transmission only when positioned within four inches of an authorized RFID reader;

(4) All contactless payment devices manufactured for distribution in the United States shall be capable of interrogation only by RFID readers contained in POS terminals at the place of business of persons authorized to accept an issuers' contactless payment devices for payment transactions;

(5) All persons accepting contactless payment transactions and all persons offering loyalty or other marketing programs shall interrogate customers' contactless payment devices using only authorized RFID readers that encrypt data transmitted to or collected from customers' contactless payment devices with at least 128-bit and triple DES encryption;

(6) Persons accepting contactless payment transactions or offering loyalty or other marketing programs shall use only authorized RFID readers capable of interrogating customers' contactless payment devices from distances no greater than four inches;

(7) Any individual's use of a contactless payment device shall be voluntary and shall not be compelled by any other person;

(8) Any individual who chooses not to use a contactless payment device for any payment transaction or loyalty or other

marketing program transaction shall not be denied service by any other person, and shall not be denied the opportunity to purchase any good or service by any other person;

(9) No person shall interrogate or attempt to interrogate any individual's contactless payment device for any purpose other than to complete an authorized payment transaction or customer-authorized loyalty or other marketing program transaction;

(10) Any person offering loyalty or other marketing programs that access and use nonpublic personal information stored on or transmitted by any consumer's contactless payment device shall access and use such nonpublic personal information only for that person's internal business purposes;

(11) No nonpublic personal information collected by a person from any individual's contactless payment device, including the device's EPC, or from any contactless payment device transaction shall be shared with any other person, including affiliated persons;

(12) Any person accepting contactless payment transactions, and any person offering loyalty or other marketing programs that access and use nonpublic personal information stored on or transmitted by any customer's contactless payment device, shall clearly notify each customer how his or her nonpublic personal information will be accessed and used for that person's internal business purposes before accessing and using any such nonpublic personal information;

(13) Any person offering loyalty or other marketing programs that access and use nonpublic personal information stored on or transmitted by any customer's contactless payment device shall require customers to opt-in voluntarily to participate in such loyalty or other marketing programs;

(14) Any person offering loyalty or other marketing programs that access and use nonpublic personal information stored on or transmitted by any customer's contactless payment device shall only interrogate a customer's contactless payment device while the customer is on the premises of the person's business;

(15) No person accepting authorized payment transactions made with contactless payment devices shall permit any affiliated or non-affiliated person to place, temporarily or permanently,

any RFID reader on its premises for any purpose, including accessing and using or attempting to access and use the nonpublic personal information stored on or transmitted by any individuals' contactless payment device;

(16) No person offering loyalty or other marketing programs of any kind shall permit any affiliated or non-affiliated person to place, temporarily or permanently, any RFID reader on its premises for any purpose, including accessing and using or attempting to access and use the nonpublic personal information stored on or transmitted by any individuals' contactless payment device;

(17) Any person collecting any individual's nonpublic personal information from any contactless payment device and storing such information in any database in any medium shall implement strict data security controls: for example, instituting multiple, layered logins plus physical confirmation of biometric authenticators to access any data; permitting data access only to bonded persons; submitting to audits by the Office of the Comptroller of Currency, FTC, or other appropriate regulatory agency, at least quarterly, to ensure compliance with required data security controls; and reporting and repairing data security breaches pursuant to any applicable federal and state laws; and

(18) Any person collecting any individuals' nonpublic personal information from any contactless payment device and storing such information in any database in any medium shall destroy all such information no later than 120 days after the collection of such information.

CONCLUSION

Contactless payment devices are an RFID application whose time is due, promising greater convenience for consumers and greater profitability for banks and merchants. While rapid, creative advances have been made by issuers of contactless payment systems, neither privacy advocates nor lawmakers have used the same creative vision to recognize the privacy problems caused by contactless payment systems. Legislation clearly delineating privacy rights in this area would serve to make applications developed for contactless payment systems more acceptable to consumers and would speed their widespread adoption. The time has come to recognize and discuss privacy problems caused by

contactless payment systems and to develop and implement appropriate privacy protections.

SHANE L. SMITH*

* J.D. 2006, William & Mary Law School; B.B.A. in Marketing 1988, West Texas A&M University. Previously, Manager, eCommerce Marketing, Valero Energy Corporation, San Antonio, Texas. I owe special thanks to my wife and best friend, Heather, and our children, Arralyn, Emily, and Landon, for their undying support and cheerfulness through three years of law school and one "lost summer" preparing for the bar exam, and to Professor Rebecca Hulse for her tireless enthusiasm, encouragement, and valuable guidance on this project.