MOBILE PAYMENTS:
CONSUMER BENEFITS & NEW PRIVACY CONCERNS

Chris Jay Hoofnagle
Jennifer M. Urban
Su Li

Mobile Payments: Consumer Benefits & New Privacy Concerns

Chris Jay Hoofnagle*, Jennifer M. Urban† & Su Li‡
BCLT Research Paper§
April 24, 2012

* Chris Jay Hoofnagle is a Lecturer in Residence at UC Berkeley Law and Senior Staff Attorney to the Samuelson Law, Technology & Public Policy Clinic.
† Jennifer M. Urban is Assistant Clinical Professor of Law at UC Berkeley Law, and Director of the Samuelson Law, Technology & Public Policy Clinic.
‡ Dr. Su Li is Statistician of Empirical Legal Studies at UC Berkeley Law.
§ The underlying survey research for this paper was fully funded by Nokia, Inc. as part of an unrestricted research gift to the Berkeley Center for Law and Technology. The cover image is Marcus Licinius Crassus by WikiMedia Commons user cjh1452000.

Introduction: mobile payments shift the privacy landscape

Payment systems that allow people to pay using their mobile phones are promised to reduce transaction fees, increase convenience, and enhance payment security. New mobile payment systems also are likely to make it easier for businesses to identify consumers, to collect more information about consumers, and to share more information about consumers' purchases among more businesses. While many studies have reported security concerns as a barrier to adoption of mobile payment technologies, the privacy implications of these technologies have been under examined. To better understand Americans' attitudes towards privacy in new transaction systems, we commissioned a nationwide, telephonic (wireline and wireless) survey of 1,200 households, focusing upon the ways that mobile payment systems are likely to share information about consumers' purchases.

We found that Americans overwhelmingly oppose the revelation of contact information (phone number, email address, and home address) to merchants when making purchases with mobile payment systems. Furthermore, an even higher level of opposition exists to systems that track consumers' movements through their mobile phones.

Below we explain some advantages of mobile payment systems, some challenges to their adoption in the United States, and then turn to our main finding: Americans overwhelming reject mobile payment systems that track their movements or share identification information with retailers. We then suggest a possible remedy for such information sharing: adapting provisions of California's Song-Beverly Credit Card Act, which prohibits merchants from requesting personal information at the register when a consumer pays with a credit card, to mobile payments systems. Our survey results suggest that consumers would support limitations on information collection and transfer. Song-Beverly could be adopted to accommodate those who wish to share their transaction data.

Benefits of mobile payments

Mobile payment technologies could bring many benefits to consumers and merchants. Mobile payment systems could act as a digital wallet, storing coupons and loyalty information. These systems may even be able to "find" and offer coupons to the consumer.

Because of the growing storage and computing capacity of mobile phones, they could also become repositories for our purchases. Mobile payment technologies could help customers keep purchase records, and could address the problem of lost receipts and rejected returns.

There is also the potential for better payment security. In most credit card transactions, consumers use the same number over and over again to effectuate charges, without a Personal Identification Number (PIN). Neither consumers nor companies can possibly ensure that the array of individuals who handle credit card numbers keep them securely. Mobile payment technologies could leverage information about the consumer, location information, security features on the device, and one-time account identifiers to more effectively verify buyers' identifies, thereby achieving more secure transactions. Properly implemented, such advances could reduce the harm created by stolen credit card numbers and make it more difficult to engage in in-person credit card fraud.

In a best-case-scenario adoption, mobile payment systems will reduce the overall cost of transactions. Currently, credit card transactions (and their generous frequent-flyer, cashback, and related rewards) are supported by merchants and consumers who pay with cash. Fees absorb two to three percent of the money exchanged in a credit transaction. To take one example of the effect of this cost, interchange fees represent the second highest expense (after payroll) at Target stores.[5]

---

[5] Andrew Martin, *Card Fees Pit Retailers Against Banks*, NEW YORK TIMES, Jul. 16, 2009, at B1.

New mobile payment systems, however, could directly pull funds from consumers' bank accounts, thus eliminating credit risk and its attendant fees (and other costs) for merchants. This could make transactions more efficient, leading to discounts or lower prices.

Still, challenges to mobile payment adoption remain

Many challenges yet remain to the adoption of new payment systems. At the most basic level, mobile payment providers must sell the system to both merchants and consumers simultaneously. Providers must convince merchants to build infrastructure at the point of sale. To do so, they must persuade enough consumers to adopt mobile payments that merchants find the system profitable.

This chicken-and-egg problem in merchant and consumer adoption leads providers to leverage existing services, such as credit card networks or carrier billing, to effectuate the actual payment. These existing services are owned by sophisticated and powerful companies that may be resistant to change. Combined, these challenges make it very difficult for new actors to start a competing, independent payment network that is more than an enhancement to an existing payment system.

One key strategy to surmount the adoption challenges on the merchant side is to leverage mobile payment systems' new capabilities for the collection and use of consumer personal information. As explained further below, traditional cash- and credit-card-based systems provide relatively limited customer information to these parties at the point of sale. Mobile payment technologies offer the ability to collect more information than before, and share it with different participants in transactions, providing an attractive service enhancement to both merchants and payment providers.

Enhancing customer information collection would also, however, raise privacy issues and attendant consumer concerns. Several researchers have examined privacy attitudes in the context of mobile payments. Most of these studies were performed outside the United

States, but nevertheless help explain the high level of rejection we discuss later in this paper. For instance, a study of consumers in Germany identified confidentiality of data as the most important concern with mobile payments, even outweighing the concern that such systems will impose direct costs upon the consumer.[6] A majority in the same study indicated that anonymity in transactions was a key function serving consumers' overall interest in confidentiality. Similarly, a focus group study of Finnish consumers in 2001 and 2002 found that, "some of the respondents were unwilling to trust their personal information with the payment service providers. They were concerned that their purchases would be tracked or that they would begin to receive a lot of advertisements."[7] As such, there is some existing evidence that consumer privacy concerns may pose a barrier to mobile payment system uptake.

Mobile payment systems raise new, unique privacy risks

To gain a fuller understanding of the new privacy issues in mobile payments, one needs to be familiar with the information flows in a standard credit card transaction.

In a typical credit card transaction, all parties to the transaction get an incomplete view of the sale.

The merchant collects information about what the consumer bought (Stock Keeping Unit (SKU) information, known as "Level 3" data) and the name of the consumer. In most cases, this Level 3 data is not transferred to any other participant in the transaction. Despite knowing what the consumer actually bought, merchants are

---

[6] K. Pousttchi, *Conditions for Acceptance and Usage of Mobile Payment Procedures*, *in* Giaglis, G. M.; Werthner, H.; Tschammer, V.; Foeschl. K.: MBUSINESS 2003 - The Second International Conference on Mobile Business. Vienna 201-210 (2003).

[7] Tomi Dahlberg, Mallat Niina & Öörni Anssi, *Trust Enhanced Technology Acceptance Model - Consumer Acceptance of Mobile Payment Solutions*, Presentation at Stockholm Mobility Roundtable Stockholm Sweden May 2223:10 (2003), available at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.200.7189&rep=rep1&type=pdf.

practically limited in using that information, because they often cannot uniquely identify their customers. Names are not unique, and thus merchants cannot use credit card swipes alone to create a reliable consumer database, with individuals tied to their Level 3 purchase histories. This is one reason why many merchants use loyalty cards. Loyalty cards allow the merchant to uniquely identify the consumer even where she uses different methods of payment.[8]

The payment network (including, for instance, Visa, MasterCard, and American Express) receives very little information from the transaction. The payment network itself may only receive the account number, the amount of the charge, and the merchant's identity.

The banks involved (the merchant's and consumer's banks), typically only receive similar information to the payment networks: the total amount of the purchase, where the purchase was made, and the consumer's unique identity (in case of the consumer's bank). Airline and hotel reservations are a common exception to this limited information transfer. In many cases, reservation information is transferred back to the consumer's bank and appears on her bill.

New mobile payment systems may disrupt these arrangements by enabling merchants to collect personally-identifiable contact information from consumers, and by transferring Level 3 data to payment networks. With these capabilities, all of the service

---

[8] Merchants may also employ other consumer reidentification systems, for example, where other information is requested from the consumer (such as zip code) at the point of sale and used to uniquely identify the consumer. See e.g. *Pineda v. Williams-Sonoma Stores*, 51 Cal.4th 524, 2011 WL 446921 (2011)(The store collected consumers' names from credit card swipes, requested the zip code, and then: "Defendant subsequently used customized computer software to perform reverse searches from databases that contain millions of names, e-mail addresses, telephone numbers, and street addresses, and that are indexed in a manner resembling a reverse telephone book. The software matched plaintiff's name and ZIP code with plaintiff's previously undisclosed address, giving defendant the information, which it now maintains in its own database. Defendant uses its database to market products to customers and may also sell the information it has compiled to other businesses.")

providers in the payments ecosystem—merchants, payment networks, and the banks involved in the transactions—could develop much more comprehensive and detailed dossiers about consumer purchase behavior than they typically have today. The capabilities of new payment systems will, for example, make it easier for merchants to build customer databases without resorting to loyalty cards.

This possible shift has profound consequences for consumer privacy and the relationship consumers have with payment providers and merchants. The need for loyalty cards will be eliminated, but so too could the ability of individuals to avoid profiling. Many consumers have long been uncomfortable with information collection surrounding their purchases. Such information collection could cause embarrassment, lead consumers to avoid buying certain items, or possibly contribute to systems that institute widespread service and price discrimination.[9]

A rise in telemarketing and commercial email?

Beyond profiling more generally, sharing contact information at the register exposes the consumer to the specific legal and practical risks of receiving more telemarketing and spam.

Most anti-marketing laws have "established business relationship" exceptions, allowing the merchant to call a customer even if that person is on the Telemarketing Do-Not-Call Registry. An established business relationship generally does not require a sale—it can be created if a consumer merely makes an inquiry at a merchant.[10]

Many merchants have not taken advantage of this exception for most consumers because they cannot prove that a business relationship exists with a specific person. If merchants are incorrect and start sales calls to a consumer, they can be sued for significant damages

---

[9] Oscar H. Gandy, Jr., THE PANOPTIC SORT: A POLITICAL ECONOMY OF PERSONAL INFORMATION. CRITICAL STUDIES IN COMMUNICATION AND IN THE CULTURAL INDUSTRIES (Westview 1993).

[10] 16 C.F.R. § 310.2(n).

under the Telephone Consumer Protection Act.[11] Thus, merchants need to ensure that they both have a business relationship, and are contacting the right consumer.

The richer data provided to the merchant in some versions of mobile payment systems could change this dynamic entirely. If mobile payment systems transfer contact information to the merchant, then the general exception for "established business relationships" will be triggered, and the merchant is more likely to start sales calls or emails.

The network will know more about consumer purchases

Beyond merchants, the payment network itself could also receive more information. Some of the companies most likely to be successful in mobile payments have designed their systems to collect Level 3 data about consumers' purchases (for example, PayPal, Google Checkout, and Facebook Credits appear to work this way).[12]

---

[11] 47 U.S.C. § 227.

[12] For example, Google Checkout's privacy policy (which is the same as its Google Wallet policy) states:

> Transaction information - When you use the Processing Service to conduct a transaction, we collect information about each transaction, including the transaction amount, *a description provided by the seller of the goods or services being purchased*, the names of the seller and buyer and the type of payment used. We may also collect transaction data from your use of the Mobile Wallet. For example, if you use the Mobile Wallet Application to make a purchase at a merchant or download a merchant coupon, we may obtain information regarding that transaction from the Mobile Wallet Application, from the merchant and/or a partner, as applicable. The information may include the date and time of the purchase, the store location, the amount of the purchase, and the offer associated with the transaction.

Google Wallet Privacy Policy, https://checkout.google.com/files/privacy.html?gl=US&hl=en (last visited April 24, 2012)(emphasis added). Google does state in an FAQ that its current NFC Wallet product does not collect Level 3-type data: "Google Wallet does not currently receive data about what products you purchase using the mobile NFC-powered app." We are not certain why these statements differ for the Mobile Wallet versus the NFC Wallet app, but we note that the Privacy Policy appears to allow collecting Level 3 data at any time.

Under existing privacy rules, these entities could share this information with third parties—for example, advertisers—without the affirmative consent of the consumer. They could also use it for their own marketing, research, or other purposes. For instance, social network services with payment systems could add transaction histories to their already rich databases of behavioral information.

Thus, a move to mobile payments could carry with it a move to a profoundly different relationship between customers and payment system service providers than has existed in the past. Further, there is no guarantee that this shift would be apparent to consumers using mobile payments systems to complete sales transactions.

Survey results

In order to learn more about consumers' privacy attitudes concerning mobile payments and privacy, we commissioned a nationwide, telephonic survey of Americans. We formulated questions to reflect the probable design of mobile payments systems, based on current vendor behavior and plans for embedding the advantages we described above into the new systems.

Overall, Americans strongly reject systems that would track them as they browsed stores and those that would share personal information with the merchant at the register.

Tracking consumers as they browse

During last season's "Black Friday," some shopping centers proposed to capture signals from consumers' wireless phones to track them as they shopped and walked through the mall.[13] These proposals quickly

[13] Sean Gallagher, *We're watching: malls track shopper's cell phone signals to gather marketing data*, ARS TECHNICA, Nov. 2011, available at http://arstechnica.com/business/news/2011/11/were-watching-malls-track-shoppers-cell-phone-signals-to-gather-marketing-data.ars

became controversial, and two shopping centers that enrolled in a tracking plan cancelled them.[14]

Collecting such information from wireless phones may violate the federal Pen Register Act.[15] Still, other companies are exploring ways to track individuals uniquely through signals emitted from phones. One system developed by Euclid tracks consumers through the "MAC address" that uniquely identifies a smartphone.[16] The MAC (for "Media Access Control") address is transmitted whenever the consumer has WiFi enabled. Similarly, Navizon I.T.S. claims that it can track, "any Wi-Fi enabled smart phone or tablet, including iPhones, iPads, Android devices, BlackBerry, Windows Mobile, Symbian and, of course, laptops."[17] As with many other tracking technologies, it seems to be designed to operate without the knowledge of the individual. Navizon claims, "Unobtrusive surveillance / Navizon I.T.S. works in the background, quietly and unobtrusively locating Wi-Fi- enabled devices…No application is needed on the devices to be tracked. The only requirement is that their Wi-Fi radios be turned on, which is the default in most smart phones, tablets and laptops."[18]

If information about the phone is combined with other data, it is very likely that individuals will be identified based upon attributes of their phones. There is concern, for instance, that individuals can be monitored and identified through unique IMSI (for "International Mobile Subscriber Identity") numbers, which, like MAC addresses, are embedded in users' phones and are transmitted during normal use of the device. In order for consumers to prevent tracking based

---

[14] Annalyn Censky, *Malls stop tracking shoppers' cell phones*, CNN MONEY, Nov. 28, 2011, available at http://money.cnn.com/2011/11/28/news/economy/malls_track_shoppers_cell_phones/index.htm.

[15] 18 U.S.C. § 3121.

[16] EUCLID, HOW DO WE COLLECT INFORMATION, Aug. 3, 2011, available at http://euclidelements.com/how-do-we-collect-information.

[17] NAVIZON, TRACK WI-FI ENABLED DEVICES INDOORS WITH FLOOR/ROOM-LEVEL ACCURACY, available at http://www.navizon.com/its.php.

[18] *Id.*

upon these technologies, they must either disable the WiFi on their phones (in the case of MAC address tracking) or turn off their phones entirely (if IMSI catchers are being employed).

We asked Americans whether they thought that phones should share information with stores when they visit and browse without making a purchase. Overwhelmingly, subjects rejected this possibility. Ninety-six percent objected to such tracking, with 79 percent stating that they would "definitely not allow" it and 17 percent stating that they would "probably not allow" it.

Sharing information at point of sale with merchants

As explained above, retailers presently receive very little information about the consumer when she pays with a credit card or cash. Merchants are restricted in how they can collect data about consumers at the register, both through credit card acceptance agreements and by practical considerations.

Mobile payments systems, however, could be configured to automatically convey uniquely consumer-identifying information to the retailer at the point of sale for later marketing or analytics use. We asked Americans about their preferences for being identified to the merchant through mobile payments systems—specifically, whether they would be willing to have their phone number, email address, or postal mail address shared with retailers.

We found that 81 percent[19] objected to the transfer of their telephone number to a store where they purchase goods. Only 15 percent would "probably allow" such sharing, and three percent would definitely allow it.

Consumers' home addresses seem to be just as sensitive as their telephone numbers. Eighty-one percent[20] said that they either

[19] Specifically, 65 percent stated that they would "definitely not allow" this sharing; 16 percent would "probably not allow" it.
[20] Specifically, 66 percent stated that they would "definitely not allow" this sharing; 15 percent would "probably not allow" it.

definitely or probably would not allow sharing of their home address with a retailer. Similar to phone numbers, only 14 percent would probably allow such sharing, and three percent would definitely allow it.

While opposition to information sharing at the register is strong in all categories we analyzed, email sharing seems to be the least sensitive category. Thirty-three percent would be willing or probably willing to share email addresses at the register. Still, 51 percent stated that they would definitely not allow their emails to be shared, and 16 percent stated that they probably would not allow it.

Likelihood of adoption

We found that over three-quarters (74 percent) of Americans said that they are "not at all likely" or "not too likely" to adopt mobile payment systems. Just 24 percent say that they are likely to adopt mobile payments.

The Federal Reserve recently published statistics on mobile payments, finding that, "Mobile payments are disproportionately used by younger consumers…Individuals age 18 to 29 account for 37 percent of mobile payment users relative to 22 percent of all mobile phone users, while individuals age 30 to 44 account for a further 36 percent of mobile payment users relative to 27 percent of all mobile phone users."[21]

We looked at a related issue—likelihood of adoption of mobile payments. We found that respondents' inclination of adopting mobile payments varies by age. The age difference overall is statistically significant (p=0.000), though no age cohort exhibits a majority that expresses likelihood to adopt the technology. Those most enthusiastic about the technology are in the 35-44 age range (16%

[21] Matthew B. Gross, Jeanne M. Hogarth & Maximilian D. Schmeiser, *Consumers and Mobile Financial Services*, Federal Reserve Board Survey (Mar. 2012), available at http://www.federalreserve.gov/newsevents/press/other/20120314b.htm.

are “very” and 21% “somewhat” likely to adopt the technology). Our oldest cohorts (55-64 and 65+) both were less likely to adopt mobile payments than other age cohorts (only 4% are “very” and 6% “somewhat” likely to adopt) and more likely to reject them (76% “not at all likely to adopt” the technology).

Age and privacy of mobile payments

Consumers’ willingness to be tracked in stores through their wireless phones, and to share phone numbers, email addresses, and home addresses with stores, varies by age. But this is significant only for some categories. For example, the willingness to share one’s home address—roundly rejected across all age groups—does not differ significantly by age, while the willingness to share email address does. It is important to note that generally, there is overwhelming opposition to all of these schemes.

While all age cohorts reject the idea of sharing phone numbers with stores where a purchase has been made, the level of rejection varies, becoming, in general, more intense with age. There appears to be a slight bend in this age trend—again, the 35-44 age group rejects the idea the least (77% said “probably” no or “definitely” no), and is most likely to answer “definitely” or “probably” yes to sharing phone numbers with merchants. However, these differences are not statistically significant and all groups reject sharing at around 80 percent.

Of all the types of personal information we inquired about, consumers were most willing to share their email addresses with stores. While majorities in every age group still rejected this sharing, rejection was somewhat less intense than for phone numbers, especially for people under 45 years old. This question, in fact, produced the biggest difference among age groups of all three types of personal information we asked about. People 18-24 years old are significantly ($p=0.002$) more likely to share email addresses with stores than other age groups, with 41 percent answering that they would “definitely” or “probably” allow this. Further, there is a noticeable split between

people 44 and younger and people 45 and older, with the younger people significantly (p=0.001) more likely to allow email sharing.

Large majorities of consumers in every age group rejected the idea of mobile payment systems sharing home addresses with merchants; here, differences between age cohorts were not significant. Overall, 81 percent of consumers said that they would "probably" or "definitely" not allow home address collection.

Even larger majorities rejected the idea of phones sharing information with stores when consumers are simply browsing, as attempted during the "Black Friday" initiative we describe above. Ninety-six percent of those surveyed rejected this option, with more than 90 percent of every age group answering that they would "probably" or "definitely" not allow it.

Identification restrictions in California law recognize consumers' concerns, but are too business-practice specific to be applicable here

In the 1980s, some merchants routinely asked consumers to share their addresses and other contact information when they paid with a credit card. This raised several privacy concerns. Cashiers might use the information to stalk customers, or to steal their identities. More broadly, there was concern that consumers mistakenly believed that they had to provide this information in order to pay with a credit card, and thus that consumers were unwittingly participating in the creation of direct marketing databases about their purchases. For instance, in 1992 the New York Attorney General reached a settlement with American Express for profiling customers into direct marketing databases, including (from low to high-end), "value seeker," "fashion conscious," "Fifth Avenue sophisticated, and "Rodeo Drive chic."[22] Former New York Attorney General Robert Abrams declared, "A consumer who pays with a credit card is entitled to as much privacy as one who pays by cash or check…Credit cardholders should not unknowingly have their spending patterns and

[22] *A Tighter Reign on Credit Data for Marketing Urged*, 2 CREDIT RISK MANAGEMENT REPORT v. 11, May 25, 1992.

life styles analyzed and categorized for the use of merchants fishing for good prospects."[23]

With similar concerns in mind, the California Legislature prohibited merchants from requiring personal information in credit card[24] transactions at the register 1990, in amendments to the Song-Beverly Credit Card Act.[25] The statute's "overriding purpose was to 'protect the personal privacy of consumers who pay for transactions with credit cards.'"[26] Specifically, the Legislature wished to prohibit businesses from, "requiring information that merchants, banks or credit card companies do not require or need."[27] Within a year, the Legislature found it necessary to strengthen the law, prohibiting merchants from even *requesting* personal information in credit card transactions.[28]

---

[23] Peter Pae, *American Express Co. Discloses It Gives Merchants Data on Cardholders' Habits*, WALL STREET JOURNAL, May 14, 1992, page A3.

[24] "Credit card" means "any card, plate, coupon book, or other single credit device existing for the purpose of being used from time to time upon presentation to obtain money, property, labor, or services on credit." Cal. Civ. Code § 1747.02.

[25] 1990 Cal ALS 999; 1990 Cal AB 2920; 1990 Cal Stats. ch. 999. These provisions were added to the Song-Beverly Credit Card Act of 1971.

[26] *Pineda v. Williams-Sonoma Stores, Inc.*, 51 Cal. 4th 524, 246 P.3d 612, 120 Cal. Rptr. 3d 531 (Feb. 10, 2011), *quoting* Assem. Com. on Finance and Ins., Analysis of Assem. Bill No. 2920 (1989–1990 Reg. Sess.) as amended Mar. 19, 1990, p. 2 ("The Problem…Retailers acquire this additional personal information for their own business purposes — for example, to build mailing and telephone lists which they can subsequently use for their own in-house marketing efforts, or sell to direct-mail or telemarketing specialists, or to others.")

[27] *Pineda v. Williams-Sonoma Stores, Inc.*, 51 Cal. 4th 524, 246 P.3d 612, 120 Cal. Rptr. 3d 531 (Feb. 10, 2011), *quoting* (Assem. Com. on Finance and Insurance, Analysis of Assem. Bill No. 2920 (1989-1990 Reg. Sess.) as amended Mar. 19, 1990, p. 2.).

[28] 1991 Cal ALS 1089; 1991 Cal AB 1477; 1991 Cal Stats. ch. 1089; see also *Florez v. Linens 'N Things, Inc*. 108 Cal.App.4th 447,453 (2003)("The obvious purpose of the 1991 amendment was to prevent retailers from 'requesting' personal identification information and then matching it with the consumer's credit card number.").

While the statutory text suggests that mobile payment technologies would be subject to the privacy provisions of the Song-Beverly Act as it now stands,[29] the Act was designed to address *merchants'* demands for information. It does not speak to how payment networks themselves could design systems to automatically collect data about the consumer. Thus, as is the case with many other sectoral-specific privacy laws, changes in technology can circumvent hard-won consumer protections.

Identification restrictions in California law, if modified, could provide a model applicable to mobile payments

Given our finding that consumers overwhelmingly reject the collection of personal information at the point of sale via mobile payment systems, we think that the Song-Beverly model should be updated to cover payments systems as well as merchants at the point of sale. [30] Song-Beverly's restrictions are particularly strict, completely foreclosing the ability of the merchant to ask for information at the register. Strict rules were necessary, because as explained above, merchants continued to elicit personal information from consumers in clever ways, culminating in the zip-code reidentification system challenged in *Pineda*.

---

[29] It broadly defines "credit card" to include "single credit device[s] existing for the purpose of being used from time to time upon presentation to obtain money, property, labor, or services on credit." Cal. Civ. Code § 1747.02. This definition mirrors Regulation Z. 12 C.F.R. § 226.2(a)(15). A supplement to Regulation Z provides examples of "credit cards," but none addresses mobile payments. *See* 12 C.F.R. pt. 226, Supp. 1 § 226.2(a)(15). The language "from time to time" concerns payment technologies can be used multiple times, as opposed to checks and "similar instruments that can be used only once to obtain a single credit extension…" 12 C.F.R. pt. 226, Supp. 1 § 226.2(a)(15)(1).

[30] Further, it may be useful to clarify that the updated law clearly covers non-paper-based transactions. Although we think this likely is a mistaken reading of Song Beverly, at least one federal district court, in a pair of cases, recently interpreted Song-Beverly to apply only to "pen-and-paper" transactions, and not "electronic entry of numbers on a keypad or touchscreen." *Salmonson v. Microsoft Corp.*, 2012 U.S. Dist. LEXIS 4632 at 4-5 (C.D. Cal. Jan. 6, 2012); *see also Mehrens v. Redbox Automated Retail LLC et al.*, 2012 U.S. Dist. LEXIS 4632 at 5 (C.D. Cal. Jan. 6, 2012).

If control over the decision to share transactional information is firmly in the hands of the user, it stands to reason that rules could be crafted to allow more liberalized information sharing. Rules could allow those who wish to share transactional data with merchants or others. An opt-in standard on a per-transaction basis could empower consumers to share where they find it appropriate but block this information collection and sharing by default. To make these protections meaningful, the decision to share must truly be voluntary. Merchants should not be able to imply that information sharing is required, or otherwise condition the provision of products or services.[31]

While the technology has shifted such that payments operators could also play the role of the 1980s information-demanding merchant, the issue remains the same: consumers' unwitting participation in contributing to detailed purchase profiles at the point of payment. Indeed, mobile payments systems could be designed to give *less* notice to the consumer, as identification, address, and Level 3 data could automatically be collected, aggregated, and shared, without the customer being actively asked for the information, at all. This model would also level the playing field between credit card, cash, and mobile transactions, and make it less likely that consumers' personal information will stand in as the value exchange in place of fees.

The broad agreement we found among Americans that they value privacy at the point of sale, suggests strong support for a modified version of Song-Beverly at the federal level. This would ensure that all Americans' expectations for privacy in their point-of-sale data are respected, and that payments systems operators and merchants alike have one, uniform regulatory model for handling point-of-sale information.

[31] We have not yet worked out an optimal model for this. We intend to take up the question of intervention in the mobile payments ecosystem in more detail in a future paper.

Methods

The Berkeley Consumer Privacy Survey obtained telephone interviews with a nationally representative sample of 1,203 adult internet users living in the continental United States. Telephone interviews were conducted by landline (678) and cell phone (525, including 235 without a landline phone). Overall, 6,906 working landlines and 8,688 working cell phones were dialed. The response rate for the landline samples was 16 percent. The response rate for the cellular samples was 14 percent.

The survey was conducted by Princeton Survey Research Associates International (PSRAI), and was fully funded by Nokia, Inc. as part of an unrestricted gift to the Berkeley Center for Law and Technology. The content of the survey was entirely composed by Berkeley Law's Chris Jay Hoofnagle & Jennifer M. Urban. Interviews were done in English by Princeton Data Source from January 27-February 12, 2012. Statistical results are weighted to correct known demographic discrepancies. The margin of sampling error for the complete set of weighted data is ± 3.4 percentage points.

Survey questions

Companies are developing new systems that would let consumers pay for items with their cell phones. These systems would let you use your phone like a credit card. How likely are you to use such a system ….(READ)

Based on cell phone owners (n=1119)

9	Very likely
15	Somewhat likely
19	Not too likely OR
55	Not at all likely?
1	Don't know/Refused

If you decided to start using your cell phone to pay for items, would you definitely allow, probably allow, probably NOT allow, or definitely NOT allow this service to (INSERT. READ AND RANDOMIZE ITEMS B-D). What about (INSERT NEXT ITEM)?

READ AS NECESSARY: Would you definitely allow, probably allow, probably NOT allow, or definitely NOT allow this?

Based on cell phone owners (n=1119)

	Definitely allow	Probably allow	Probably not allow	Definitely not allow	DK/Ref.
a. Share information about you with the stores that you visit, when you are just browsing	1	3	17	79	*
b. Share your phone number with the stores where you make purchases	3	15	16	65	*
c. Share your email address with the stores where you make purchases	6	27	16	51	1
d. Share your home address with the stores where you make purchases	4	14	15	66	1