

# Mobile Payments Can Expose More Consumer Data and Weaken Privacy Laws

by [Harley Geiger](#) [1]  
April 23, 2012

Get ready for mobile payments to change how we make in-store purchases and how companies collect information about us. Nearly all the major smartphone manufacturers, mobile network operators, credit card issuers, and tech companies are [gearing up](#) [2] to provide consumers with mobile payment services. Many of these services will let consumers buy items in brick-and-mortar stores just by [swiping](#) [3] their phones at checkout.

While this will create interesting and convenient new apps, mobile payments will also provide more consumer data to more companies than traditional offline credit card transactions. Without strong user privacy controls, mobile payments may [turn](#) [4] your cell phone into a magnet for telemarketing, spam, and online behavioral advertising.

(For more background on the technology and privacy issues with mobile payments, please see our earlier [blog post](#) [5].)

## More information to more companies

Mobile payment services can expose consumer data to several companies that were not included in traditional credit card transactions. In addition to credit card issuers and payment processors, mobile payment services also involve the mobile payment provider (i.e., Google, in the case of [Google Wallet](#) [6]), the mobile network operator (i.e., [Verizon or AT&T](#) [7]), and third party apps that consumers download (such as a budget app). With mobile payments, these companies can get access to the consumer information revealed during a traditional credit card transaction – and more – and use this information in new ways.

With magnetic stripe credit card transactions, credit card companies have [access](#) [8] to consumers' contact information, codes identifying the general category of purchases, as well as the date, time, location, and amount of the purchase. In addition to this data, companies can program their mobile payment systems and apps to track the specific items a consumer purchases. Today, most consumers do not expect their offline transactions to influence the advertising they see on the Internet, but consumers should expect mobile payment services to [use](#) [9] transaction information to hit consumers with offers, coupons, and customized advertising.

Merchants can get also more detailed consumer information from mobile payments than from traditional magnetic stripe credit cards. When using regular credit cards, merchants hold an itemized receipt reflecting consumers' purchases, but merchants do not receive the cardholder's full contact information – telephone number, email address, and mailing address – unless the consumer provides it to them or the merchant takes the trouble to seek out the consumer's personal information from a credit bureau. This is one major reason why merchants institute loyalty card programs, so they can match customers' purchase histories with their identifying information to create detailed profiles of the customers' shopping habits.

Many mobile payment services will collect consumers' contact information when they register with the service. Mobile payment services and apps can be programmed to provide merchants with consumers' phone numbers, email addresses, and purchase histories during a transaction in a store – so long as the merchant's point of sale system is able to receive this information. Consumers today are enrolled in loyalty programs with only a few companies, such as their supermarkets, but mobile payment services will make it simple to establish the equivalent of a loyalty program for every merchant the consumer comes into contact with – every café, taxicab company, or magazine stand. The easy ability to build detailed customer profiles is a common [incentive](#) [10] for merchants to embrace mobile payment services.

## **Weakening privacy laws**

As CDT [pointed out](#) [5] previously, mobile payment services that provide merchants with consumers' contact information will weaken the protective effect of existing privacy laws, such as those restricting telemarketing and spam.

Telemarketing:

The Telephone Consumer Protection Act (TCPA) [requires](#) [11] telemarketing companies to honor two basic types of "Do-Not-Call" (DNC) lists. The first is the wildly popular national DNC list, and the second is the internal DNC list managed by each company. Consumers can register their landline or cellular numbers with the national DNC list, and all companies are permanently [prohibited](#) [12] from calling or sending text messages to those numbers for solicitation purposes. However, this blanket prohibition does not apply to those companies with which the consumer has an "established business relationship" (EBR). An EBR is formed when a consumer buys goods or services from a seller. Many state telemarketing laws [also](#) [13] contain this EBR exception.

Because traditional credit card transactions do not reveal consumers' phone numbers to merchants, most merchants today are unlikely to make telephone or text solicitations to consumers – even when they have an EBR. However, mobile payment services and apps can be programmed to give merchants consumers' phone numbers during transactions. This frees every merchant from whom a consumer makes a purchase – no matter how small – to make telephone or text solicitations to the consumer, even if the consumer is on the national DNC list.

A consumer can restrict telemarketing calls and text messages from companies with whom she has an EBR by registering her cellular number with each individual company's internal DNC list. After the consumer gets on a company's internal DNC list, that company is prohibited from making telephone solicitations to that number for five years – regardless of whether the consumer continues to do business with the company. One downside to this process is that it requires consumers to opt in to the internal DNC list of each individual telemarketer or company from whom they make a purchase. With more companies receiving contact information due to mobile payments systems, consumers will have to rely more on internal DNC lists, increasing the burden of privacy protection on consumers and confusing those who believed the national DNC list already provided privacy protection.

Spam:

Magnetic stripe credit card transactions do not reveal consumers' email addresses, to merchants, making it somewhat difficult for merchants to send commercial email to consumers with whom they have a business relationship. However, mobile payment services can be programmed to provide a consumer's email address to a merchant during each transaction, making it easier to send commercial emails to the consumer. The CAN SPAM Act [gives](#) [14] consumers the right to opt out of commercial email messages from specific companies. A limitation of CAN SPAM, however, is that consumers must communicate the opt out to each company that sends them spam. As with telemarketing, greater reliance on the opt out provided by CAN SPAM will increase the burden of privacy protection on consumers.

Because the CAN SPAM Act is [limited](#) [15] to messages sent to addresses that use Internet domain names, the Act does not appear to offer consumers any protection from electronic advertisements that bypass email and text message systems. For example, mobile payment services with "near field communication" can enable merchants to load coupons or advertising messages directly onto the phone, using the same channel that transmits consumers' payment information to merchants.

## **'Privacy by design' is crucial**

Building strong user privacy controls into mobile payment services during the design phase is the most efficient way of addressing these problems. CDT has repeatedly [called on](#) [16] companies to integrate privacy protections into the fabric products and services, a process known as "privacy by

design.” The Federal Trade Commission’s recent [report](#) [17] on consumer privacy likewise urges companies to build privacy into their products and to provide consumers with meaningful choices regarding how information about them is shared.

Mobile payment services should give users both global and granular options to restrict the disclosure of any information that is not necessary to complete a transaction. This way, consumers can decide how much information is given or withheld from merchants, mobile payment providers, and app developers. Ideally, mobile payment services should easily allow consumers to opt out of telemarketing or commercial emails from merchants – so, for example, consumers can use their mobile phones to join a merchant’s internal DNC list at the same time that the mobile payment service completes a transaction. This solution would not require new regulation, but it would require the cooperation of mobile payment service providers, merchants, and point of sale system manufacturers. Privacy by design also does not replace the need for [baseline consumer privacy legislation](#) [18], which should encompass mobile payments.

Mobile payments can offer killer apps and great convenience to consumers. But if companies fail to build meaningful privacy controls into their services, consumers will not trust mobile payments and a promising new industry [will](#) [19] be discredited.

- 
- [NFC](#)
- [Near field communication](#)
- [mobile payments](#)

Copyright © 2013 by Center for Democracy & Technology. CDT can be freely copied and used as long as you make no substantive changes and clearly give us credit. [Details](#).

**Source URL:**

<https://cdt.org/blogs/harley-geiger/2304mobile-payments-can-expose-more-consumer-data-and-weaken-privacy-laws>

**Links:**

- [1] <https://cdt.org/personnel/harley-geiger>
- [2] <http://pewinternet.org/Reports/2012/Future-of-Money.aspx>
- [3] <http://youtube.com/watch?v=2KTyFE3sfSo>
- [4] <http://cnbc.com/id/46987269>
- [5] <http://cdt.org/blogs/harley-geiger/nfc-phones-raise-opportunities-privacy-and-security-issues>
- [6] <http://google.com/wallet/how-it-works.html>
- [7] <http://paywiththis.com/about-us.xhtml>
- [8] <http://merchantequip.com/merchant-account-blog/72/level-1-2-and-3-credit-card-processing>
- [9] <http://bloomberg.com/news/2011-05-26/google-unveils-mobile-payment-service-to-expand-in-advertising-coupons.html>
- [10] <http://www.retailtouchpoints.com/mobile/1530-mobile-wallets-and-nfc-battle-for-retailer-mindshare>
- [11] <http://law.cornell.edu/cfr/text/47/64.1200>
- [12] <http://ftc.gov/opa/2008/04/dncfyi.shtm>
- [13] <http://www3.dncsolution.com/marketing/reginfo/reginfo8.asp>
- [14] [http://www.law.cornell.edu/uscode/text/15/7704#a\\_3\\_B](http://www.law.cornell.edu/uscode/text/15/7704#a_3_B)
- [15] <http://www.law.cornell.edu/uscode/text/15/7702>
- [16] <http://cdt.org/policy/role-privacy-design-protecting-consumer-privacy>
- [17] <http://ftc.gov/opa/2012/03/privacyframework.shtm>
- [18] <https://www.cdt.org/issue/baseline-privacy-legislation>
- [19] <http://bloomberg.com/news/2012-04-30/mobile-spam-texts-hit-4-5-billion-raising-consumer-ire.html>

