

# NFC Phones Raise Opportunities, Privacy And Security Issues

by [Harley Geiger](#) [1]  
April 11, 2011

Near field communication (NFC) is coming to your phone. How do we know? Because Google, Apple, Microsoft, Sprint and you-name-it say so. When the technology will actually be widely deployed is not entirely certain, but strong signals point to this happening within the next two years. The move will open the doors to a slew of interesting applications and could transform the way we pay for merchandise at the point of sale. Incorporating NFC into smartphones – especially in the way many companies envision it – will also have distinct implications for consumer privacy and data security that may not be covered by current regulations.

## What is NFC?

[NFC](#) [2] is a form of short-range communication that wirelessly exchanges data between a reader (such as a phone or sensor) and a target (such as another reader or a microchip embedded in an object). Targets need not have a power source for readers to scan them. NFC is essentially a subset of radio frequency identification ([RFID](#) [3]) but, as the name implies, near field communication has a shorter read range – a maximum of about 20 centimeters, although it is possible to amplify this. The most common application for NFC today is to enable contactless payment with mobile phones.

Like RFID, NFC is a versatile technology and certainly not limited to mobile payments. NFC can be used for advertising, such as to download information or coupons from interactive posters or digital signage. NFC can also provide access to secure areas, such as office buildings with an NFC-activated lock. People with NFC phones could pass electronic messages to each other – like a fire bucket brigade – without the need for Internet or cellular service, by touching phones. NFC may facilitate a great variety of innovative apps – for now, though, phone software and hardware manufacturers appear to be focused on deploying NFC for mobile payments.

## Cue Battle For Marketplace Dominance

Newer versions of Google's Android mobile operating system have NFC functionality [built in](#) [4]. Google recently [confirmed](#) [5] that it partnered with MasterCard and Citigroup to develop a mobile payment system using NFC. AT&T, Verizon, T-Mobile and Barclaycard US [announced](#) [6] a mobile payment venture in late 2010 called ISIS. It is widely [rumored](#) [7] that the next generation of the iPhone will include NFC. [Microsoft](#) [8], [Sprint](#) [9], [Amazon](#) [10], [RIM](#) [11] and others are also reportedly working on incorporating NFC into their products. It seems clear that NFC is going to make waves in the handset market, but how revenues will be shared among the parties involved (carriers, handset makers, merchants, etc.) is still an [open question](#) [12].

Interestingly, a fight seems to be [brewing](#) [13] between carriers and handset makers over whether payment data should be stored in the SIM card or on the phone's embedded chip. Google's business model would bypass the SIM card entirely, and RIM [reportedly](#) [14] seeks to do the same. Storing financial information on the embedded chip could make the information more easily available to anyone with access to the chip, such as the handset maker, third party developers or merchants. This would also enable consumers to change carriers but retain the data on their phones. Carriers, however, would prefer to store the financial information on the SIM card, which could give carriers greater control over consumers' NFC transactions and may enable carriers to play broker to deals with merchants and service providers. This battle may have a substantial impact on consumers' freedom to use NFC with the merchants and developers of their choice.

## Privacy And Security Will Be Major Issues

As with credit cards, the sensitive financial data stored on mobile phones will become targets for

thieves and the unscrupulous. The upside, though, is that the [security](#) [15] of NFC-enabled phones could be quite good, or at least no worse than a credit card. Since smartphones are miniature computers, strong cryptography and authentication protocol can be built into their systems – but it is up to device manufacturers and service providers to ensure these protections are in place for NFC transactions. NFC’s relatively short read range provides some protection against eavesdropping on transactions, but it may be [possible](#) [16] to pick up data from NFC systems at a greater distance using an antenna. Of particular concern for data security are man-in-the-middle attacks in which a party to one transaction drops some form of spyware or malware onto the phone, subsequently infecting other phones that the original interacts with later. Anti-virus software and operating system architecture that controls flow of information between applications will be important safeguards to mitigate such attacks.

Unfortunately, studies indicate that most consumers do not understand current risks and are not diligent about the security of their phones. A recent Ponemon institute [survey](#) [17] found that less than half of consumers use passwords or keypad locks, only 29 percent of consumers say they have considered installing anti-virus software, and only 10 percent turn off their Bluetooth “discoverable” status when their phone is not in use. In fact, according to the Ponemon survey, consumers were more concerned about receiving unwanted marketing and promotions on their phones (67 percent) than virus attacks (44 percent). Previous studies convey similar concerns. A 2009 KPMG [study](#) [18] showed that 48 percent of consumers who have not tried mobile payments cite security and privacy as the primary reasons, and a 2007 [survey](#) [19] from the Helsinki School of Economics found consumers were concerned that mobile payment service providers would track their purchases and personal information for marketing purposes. It turns out that consumers have good reason to anticipate more mobile advertisements.

Google, Sprint and possibly others have already made clear that they do not intend to generate revenue by taking a cut of mobile payment transactions. Instead, they [hope](#) [5] to use NFC to provide highly personalized advertisements and coupons at the point of sale. Likewise, [retailers](#) [20], [digital signage companies](#) [21] and [others](#) [22] are considering ways to leverage NFC to deliver marketing tailored to location and preferences, enabling the “rich brand experience” so many companies believe consumers crave. Deep involvement by Google in mobile payments is uniquely consequential in that Google already gathers colossal quantities of data on consumers’ search habits, emails, calendars and locations. With NFC-equipped Android phones, Google will also have access to data on where individuals shop, when, and what they purchase.

### **Will A Gap In Regulation Reduce Consumer Privacy?**

Several laws can affect consumers’ privacy when it comes to mobile marketing, but these laws are not all-inclusive. The Gramm–Leach–Bliley Act ([GLBA](#) [23]) requires mobile payment service providers, as financial institutions, to allow consumers to opt out of sharing personal information for third party marketing, but not marketing by the financial institution itself. The [CAN-SPAM Act](#) [24] and the Telephone Consumer Protection Act ([TCPA](#) [25]) generally prohibit sending unsolicited commercial emails and text messages to wireless devices. However, the prohibition does not apply when a consumer has provided affirmative consent or (under TCPA) has an established business relationship with the sender of the message. Unfortunately, these protections are a poor fit for marketing related to NFC transactions.

GLBA may not apply if it is the consumer or a third party (such as an app developer) and not the financial institution that is technically disclosing personal information during NFC transactions. When a consumer uses NFC to purchase a product from a merchant, that individual presumably establishes a business relationship with the merchant, and TCPA would permit the merchant to send transactional and advertising messages to the consumer’s phone via text or email. However, it is somewhat unlikely that text messages and emails – as defined under CAN-SPAM – will be the preferred marketing channel associated with NFC.

Instead, it seems more probable that merchants will load ads, coupons or adware directly onto the phone itself during the NFC transaction, bypassing the Internet. Other service providers are more likely to use purchase information to influence the ads that appear while the consumer surfs the Internet. CAN-SPAM, TCPA and GLB do not fully cover these scenarios. It is also quite possible that

many consumers will provide consent to receive marketing messages related to NFC transactions, such as through software licensing agreements or notices provided by merchants or marketers at the point of sale.

## **A New Front In Consumer Protection**

In 2006, CDT released our [Privacy Best Practices for the Deployment of RFID](#) [26], which we developed in collaboration with some of the nation's most well-known companies and consumer advocacy groups. While NFC is not an exact fit, many of the protections CDT recommends for RFID are appropriate consumer protections for NFC mobile transactions. Among the most important are ensuring data security, providing consumers with clear notice of what their personal information will be used for, and prohibiting uses of consumers' information that are unnecessary to complete a transaction and are inconsistent with consumers' preferences. As with RFID, consumers should have a choice regarding whether their personal information is used for marketing purposes – whether by service providers, merchants or others. Consumers should have access to any individual profiles companies create based on consumers' purchasing habits.

The FTC's December 2010 [Staff Report](#) [27] recommends a strong framework for consumer privacy that companies using NFC should apply. The Staff Report centers around three main principles: privacy by design, simplified choice and greater transparency. Companies should bake in privacy protections for this emerging technology from the beginning, rather than try to retrofit safeguards onto a widely deployed existing system. Companies need to be obvious and upfront about privacy implications in ways consumers will actually notice, just not in terms and conditions. Companies also should let consumers have simple and real controls over their information, including the option to complete a transaction using an NFC-equipped mobile phone without turning over their personal information for any marketing purpose. The privacy protections companies ultimately apply should cover the full set of [fair information practices](#) [28].

## **Getting NFC Off To A Positive Start**

Industry, regulators, and consumers will have a strong role to play in ensuring NFC becomes a safe and enjoyable addition to consumer electronics. In addition to the FTC Staff Report and the CDT RFID Best Practices, companies should take care to comply with the Mobile Marketing Association's [Mobile Couponing Guidelines](#) [29]. As NFC is rolled out in force over the next couple years, regulators should observe the mobile payment ecosystem to assess whether the current mix of law and industry self-regulation adequately protect consumers. Lastly, consumers need to take steps to protect sensitive data on their mobile phones. Equipping mobile phones with NFC is an exciting development with great potential benefits, but it must not come at the expense of consumer choice, privacy and security.

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

~~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://www.cdt.org/blogs/harley-geiger/nfc-phones-raise-opportunities-privacy-and-security-issues>

### **Links:**

[1] <https://www.cdt.org/personnel/harley-geiger>

[2] <http://www.nfc-forum.org/resources/faqs#headTechnology>

[3] <http://www.rfidjournal.com/article/view/1339>

[4] <http://www.readwriteweb.com/mobile/2011/02/android-gains-more-nfc-capabilities.php>

- 
- [5] <http://online.wsj.com/article/SB10001424052748703576204576226722412152678.html>
- [6] <http://www.bloomberg.com/apps/news?pid=conewsstory&tkr=T:US&sid=azuNszZW5xG8>
- [7] <http://bits.blogs.nytimes.com/2011/03/21/mobile-payments-to-become-next-frontier-in-mobile-fight/>
- [8] <http://www.businessweek.com/news/2011-03-30/microsoft-is-said-to-plan-mobile-payments-in-ph-one-software.html>
- [9] <http://www.readwriteweb.com/mobile/2011/04/nfc-in-2011-sprint-prepares-to-take-on-isis.php>
- [10] <http://www.bloomberg.com/news/2011-03-31/amazon-com-said-to-be-considering-mobile-payment-service-for-smartphones.html>
- [11] <http://www.pcmag.com/article2/0,2817,2380419,00.asp>
- [12] [http://www.nytimes.com/2011/03/24/technology/24wallet.html?\\_r=2](http://www.nytimes.com/2011/03/24/technology/24wallet.html?_r=2)
- [13] <http://www.mobilecommercedaily.com/2011/03/21/who-owns-the-paying-mobile-consumer-carriers-or-handset-makers>
- [14] [http://www.readwriteweb.com/archives/rim\\_fights\\_carriers\\_over\\_nfc\\_iphone\\_5\\_to\\_have\\_nfc.php](http://www.readwriteweb.com/archives/rim_fights_carriers_over_nfc_iphone_5_to_have_nfc.php)
- [15] <http://whmurray.blogspot.com/2011/04/near-field-communication-nfc.html>
- [16] <http://www.proxmark.org/proxmark>
- [17] <http://www.avg.com/filedir/other/Smartphone.pdf>
- [18] <http://www.kpmg.com/US/en/IssuesAndInsights/ArticlesPublications/Press-Releases/Documents/mobile-banking.pdf>
- [19] <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.106.5746&rep=rep1&type=pdf>
- [20] <http://www.retailcustomerexperience.com/article/179765/VeriFone-to-include-NFC-in-all-new-POS-terminals>
- [21] <http://blogs.ft.com/fttechhub/2011/03/billboards-digital/>
- [22] [http://www.nfc-forum.org/news/pr/view?item\\_key=5e39864ceb2626f09eb96de8d9e7ca6a91415b3f](http://www.nfc-forum.org/news/pr/view?item_key=5e39864ceb2626f09eb96de8d9e7ca6a91415b3f)
- [23] <http://business.ftc.gov/privacy-and-security/gramm-leach-bliley-act>
- [24] <http://www.fcc.gov/cgb/consumerfacts/canspam.html>
- [25] <http://www.fcc.gov/cgb/consumerfacts/tcpa.html>
- [26] <http://www.cdt.org/privacy/20060501rfid-best-practices.php>
- [27] <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>
- [28] [http://www.dhs.gov/xlibrary/assets/privacy/privacy\\_policyguide\\_2008-01.pdf](http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf)
- [29] <http://mmaglobal.com/mobilecouponguidelines.pdf>