Mobile Near Field Communications (NFC)
"Tap 'n Go"
Keep it Secure & Private

Ann Cavoukian, Ph.D.

Information and Privacy Commissioner,
Ontario, Canada

Acknowledgements

The Information and Privacy Commissioner gratefully acknowledges the input and work of the **Nokia Privacy and NFC Teams**, as well as Ken Anderson, Assistant Commissioner of Privacy, Michelle Chibba, Director of Policy and **Fred Carter**, Senior Policy and Technology Advisor, *Office of the Information and Privacy Commissioner of Ontario, Canada* in the preparation of this paper. Special thanks also extend to **Collin Mulliner**, *Technische Universität Berlin and T-Labs,* and **Harley Geiger**, Policy Counsel at the *Center for Democracy and Technology*, for their invaluable assistance in reviewing and commenting on earlier drafts.

NFC Forum and the NFC Forum logo are trademarks of the Near Field Communication Forum

Information and Privacy Commissioner,
Ontario, Canada

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8
Canada

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca
Privacy by Design: www.privacybydesign.ca

IPR2025-01151
Apple EX1039 Page 2

Table of Contents

Introduction 1

NFC Technology Summary 2

NFC Reference Use Cases 4

1. Service Initiation – Reading a "Smart" Movie Poster 5

2. Pairing of Devices – Activating a Bluetooth Printer Connection 7

3. Peer-to-peer Data Transfer – Sharing Contact Info Between Devices 8

4. Secure NFC Card — Presenting a Loyalty "Card" 10

Applying ***Privacy by Design*** to Mitigate Risks 11

1. ***Proactive*** not Reactive; ***Preventative*** not Remedial 11

2. Privacy as the ***Default Setting*** 12

3. Privacy ***Embedded*** into Design 12

4. Full Functionality — ***Positive-Sum***, not Zero-Sum 13

5. End-to-end Security — ***Full Lifecycle Protection*** 13

6. ***Visibility*** and ***Transparency*** — Keep it ***Open*** 13

7. ***Respect*** for User Privacy — Keep it ***User-centric*** 13

Residual Security and Privacy Risks 14

Automated Linkages to Other Communications Channels 14

Inadequate User Information and Prompts 14

Poor Application Design 15

Interoperability Vulnerabilities in Device Hardware and Platforms 15

Tampering and Spoofing of NFC Tags 15

Corrupted or Malicious Tag Data 16

Emerging Environments, Infrastructures of Ubiquitous Surveillance 16

Conclusions 17

References 18

Introduction

Near Field Communications (NFC) is a short-range wireless technology that allows mobile devices to actively interact with passive physical objects and other active mobile devices, connecting the physical world to mobile services in ways that empower and benefit users. We will also be using the term "Tap 'n Go" because it clearly conveys a visual image in which this technology is intended to be used.

NFC builds upon Radio-Frequency Identification (RFID) and contactless smartcard technologies that enable stored data to be actively "read" at a distance. RFID is a powerful enabling technology that is being applied in an astonishing range of applications and uses, from supply chain management and product inventory control to identity authentication and access control. However, as RFID technologies become widely deployed, the possibility of unwanted identification, tracking and surveillance may increase, as may the likelihood of data interception, "cloning" and misuse.

"NFC" as referenced in this document, is the technology defined by the publicly-available information and specifications from the NFC Forum[1]. The NFC Forum is a global industry association that represents the interests of the NFC ecosystem[2]. NFC technology addresses some of the security and privacy concerns of RFID by restricting the physical separation of NFC devices and tags to a close proximity. Additionally, NFC includes specific reference use cases, additional technical specifications and usage profile specifications for existing standards.

In the most-common use case scenarios, users' mobile devices will scan, acquire and act upon the data available in posters and kiosks, connect and exchange data with other devices, emulate RFID tag readers to read and act on scannable coupons, vouchers, tickets and emulate a contactless card to act as a loyalty, access, or payment card. NFC builds upon the proven strengths of RFID "remote identification" technologies while addressing many of the security and privacy risks.

By applying *Privacy by Design* principles, NFC can enable privacy-respectful sharing and simplified transactions. In fact, the "Tap 'n Go" (TnG) mobile user experience of NFC acts as an extension of consumer gestures required to activate various NFC use cases, such as presenting an electronic ticket or pass, accessing a locked door, or sharing personal information.

This paper

- introduces NFC and its capabilities to potential users and the public;
- discusses the potential privacy and security risks;
- explains how some risks are presently being met; and
- introduces considerations for engineers and developers of NFC applications to embed additional security and privacy measures into the design of applications that use NFC capabilities.

1 The Near Field Communication Forum was formed to advance the use of NFC technology by developing specifications, ensuring interoperability among devices and services, and educating the market about NFC technology. See http://www.nfc-forum.org/aboutus/.

2 NFC ecosystem is described further at http://www.nfc-forum.org/aboutnfc/ecosystem/.

IPR2025-01151
Apple EX1039 Page 4

NFC Technology Summary

Developed by a global consortium, NFC is based on technology specified by numerous international standards that allows for easy transfers of information over small distances. It can turn a handset into a device for reading data attached to physical objects, be used for exchanging data between two mobile devices and be used for paying for various products, such as public transit tickets and travel cards.

As noted earlier, NFC is compatible with – and builds upon – existing RFID technologies found in millions of access, payment and identification cards – data which is accessible through an emerging RFID reader infrastructure. NFC is particularly well-suited for use in mobile devices, where its operation and behaviour are controlled by the device owners.

In the context of use with mobile devices, NFC has three principal modes of operation[3]:

Reader/Writer

This NFC mode enables mobile devices to read data stored in passive RFID tags embedded in public posters, displays, and products — and to act upon that data that contains a Uniform Resource Locator (URL), which is an Internet encoding of access instructions for a file or Web address, or instruction for making a call, or the SMS instruction for sending a text message. This NFC mode also enables mobile devices to write data to some tags – notably virtual tags in other devices.

Card Emulation

This NFC mode enables mobile device owners to make a contactless business transaction, in the same way smart cards are used today. This mode of operation enables mobile devices to be used for identification, payment and access control applications.

Peer

This NFC mode enables mobile devices to more easily interact with each other (i.e., each phone has to be equipped with NFC and the enabling applications) to quickly launch a mobile communications bearer for sharing data with each other, whether to exchange business cards, photos, documents or other type of personal information in "peer-to-peer" data transfers.

3 Refer to the Architecture section off the NFC Device Requirements 1.0 specifications at http://certification.nfc-forum.org/docs/NFC_Forum_Device_Requirements.zip

IPR2025-01151
Apple EX1039 Page 5

Yesterday's cell phones have become today's "smart" mobile devices, thanks to broadband network access to the Internet and Web and enhanced sensor, storage and processing capabilities that enable new feature and service innovations. Mobile computing devices have become ubiquitous, serving as personal travelling companions and tools for hundreds of millions of people. As such, they need to be secure, trusted and empowering.

As we wrote in 2010[4], data privacy and security must be "baked into" mobile device architectures, including physical design, operating systems, applications and services, with special attention to effective user interfaces and default privacy options. The foundation principles of *Privacy by Design* apply also to the mobile domain. All stakeholders in the mobile privacy ecosystem have critical roles to play in fostering user trust and confidence.

Mobile devices that allow for system-to-system data transfers, or pairing of devices to enable interaction, may trigger privacy concerns, including the following:

- Unwanted data leakage or collection;
- Tracking of a user's location;
- Identifying users in situations where they wish to remain anonymous;
- Improper redirection to an unknown website;
- Initiation of an unknown service; and
- Receipt of unwanted content.

However, the NFC technology and ecosystem addresses some of these privacy concerns, for example:

- NFC requires less than 4 centimetres of close proximity for interactions. At this close range, users will have foreknowledge of the person or device that they are interacting with;
- NFC interactions are based on a "tapping" consumer gesture, where both NFC devices either touch or are within a few centimetres of each other in order to initiate an NFC interaction. This makes "skimming" and "eavesdropping" very difficult[5];
- NFC capabilities should be disabled when the screen or keyboard of an NFC-enabled mobile phone is locked. Additionally, the mobile platform should permit users to disable the NFC function, as well as any alternative communication technology (e.g., Bluetooth or WiFi) used for peer-to-peer transfer of personal information. This prevents unintended NFC interactions;
- NFC implementations should provide user feedback on interaction requests from another NFC-enabled device. This reduces hidden or unwanted NFC interactions; and
- NFC-initiated sharing of personal data should be accomplished with use of regenerated identifiers, to avoid association of a device and its user with an NFC interaction.

4 See Cavoukian, *et alia*, *The Roadmap for Privacy by Design in Mobile Communications: A Practical Tool for Developers, Service Providers, and Users* (Dec 2010).

5 See http://www.nfc-forum.org/aboutnfc/tech_enabler/

IPR2025-01151
Apple EX1039 Page 6

NFC Reference Use Cases

Currently, targeted use cases utilize the NFC technology more as an input mechanism for launching other communications technologies, than as a radio type for actual data transfer. While the NFC technology supports extension mechanisms for transfer of large amounts of data, the current radio frequency allocation to NFC requires close proximity of NFC devices during interactions, which creates a user experience that is not conducive to long data transfers. This is why NFC is typically expected to be used for either small data transfer interactions or for launching larger data transfers with an alternative mobile wireless communication technology, such as Bluetooth, WiFi and mobile data service.

NFC provides a capability for initiating wireless communication interactions. There are four main reference use cases for these interactions:

1. Service initiation (e.g., read a tag on a poster and launch a Web browser to get product discount coupons);

2. Pairing of devices (e.g., activate a Bluetooth headset by tapping on the mobile accessory);

3. Peer-to-peer data transfer (e.g., quickly and easily transfer information between mobile devices with a simple touch); and

4. Secure NFC card (e.g., mobile device acts as an access, loyalty, or payment contactless smart card).

IPR2025-01151
Apple EX1039 Page 7

1 Service Initiation

Reading a "Smart" Movie Poster — True Tap 'n Go!

The Smart Poster use case enables the read/write mode to provide a simple way to access a remote service by using the "Tap 'n Go" paradigm of NFC to start a service. Similar scenarios include acquiring product item information, transit schedules, location-related data such as maps, interactive advertising material, online contest information, or mobile network links to information and other content.

Actors in use case scenario #1

- Alice, who retrieves and uses a discount voucher/coupon.
- Movie ecosystem that makes use of ad posters to promote new movie entertainment offerings to the public.
- Alice's NFC-enabled mobile device.

Description of events

1. Alice runs across an interesting poster on the street, promoting a movie and offering a discount voucher/coupon for the premiere of the movie.

2. Alice notices that the poster informs that the voucher/coupon can be acquired by tapping the poster with an NFC-enabled mobile device.

3. Alice taps the poster with her NFC-enabled smartphone.

4. Alice's phone opens an NFC application that prompts her that she is about to launch her smartphone's browser to access a website that Alice notices is specified on the poster as the site to get the discount voucher/coupon for the movie premiere.

5. Alice confirms that she wishes to access the website and, by doing so, her phone accesses the website and she receives the discount voucher/coupon on her phone.

IPR2025-01151
Apple EX1039 Page 8

6. Alice uses the voucher in the evening to get a half-price admission to see the movie premiere. This involves the movie theatre ticket office scanning the discount voucher/coupon on Alice's phone and Alice purchasing the discounted movie ticket.

Key risks for users

- RISK 1: NFC tags can be susceptible to tampering. Smart posters are located in public places, where such malicious threats are possible. The tag itself is passive and can be rewritten or superimposed with different data. A poster containing malicious information could direct Alice to a false Web service or website and, instead of transferring the voucher to the mobile device, could misguide her to perform other, unwanted purposes. Alternatively, the repurposed tag data could include a malicious URL to instruct her mobile phone to make a mobile call or send a text message to a premium service resulting in unwanted mobile billing charges. In this use case, NFC passive tag technology is being used to quickly and easily launch a communication service. This risk is shared with Internet browsers, as well as calling or texting to an unknown phone number.

- RISK 2: Alice may not have received a full understanding of what, how, why and by whom her personal information is being collected, processed, transferred or stored and how Alice could find out about it. If this notification were not provided, (explicitly in writing on the smart poster or indirectly by a reference on the poster to some online site) then Alice's actions could be lacking proper informed consent. This risk is one of (if not the) most common privacy risks to consumers. Consumers can easily be subtly encouraged to act on consumer cues, without taking proper steps to understand the potential impact of their actions.

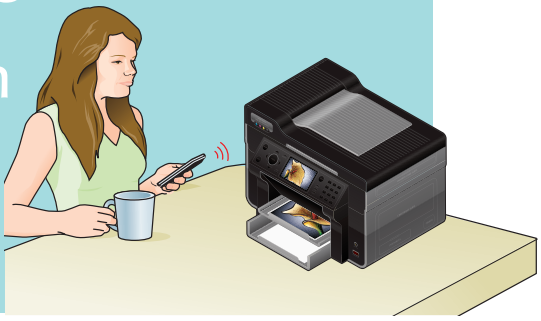
- RISK 3: As with any consumer online activity, there are risks that a malicious party may use social engineering to gather Alice's personal information without her consent. In this case, the risk is that the service initiated with the smart poster tag could have secondary, hidden purposes to which Alice has not given consent. Such threats could undermine consumer trust in a digital marketplace.

- RISK 4: Alice may have unknowingly leaned up against the smart poster with her smartphone in her hand, while talking on the phone or idly standing by. If NFC-capability in her phone is active at the same time, Alice may inadvertently activate the interaction contained in the smart poster passive tag.

IPR2025-01151
Apple EX1039 Page 9

2 Pairing of Devices

Activating a Bluetooth Printer Connection



The Pairing of Devices use case enables the read mode to provide a simple way to pair and connect two NFC devices. Similar scenarios include pairing with home multimedia center, in-car audio, headsets, cameras and digital frames.

Actors in the use case scenario #2

- Alice, who wants to print her camera phone photos on a publicly accessible printer.
- Mobile device with NFC and Bluetooth connectivity capability.
- NFC-enabled Bluetooth printer.

Description of events

1. Alice finds it difficult to connect her mobile device with other Bluetooth-enabled devices but understands that NFC technology can simplify such connections.

2. Alice sees the NFC logo on a Bluetooth-enabled color printer, indicating its capability and compatibility for quick pairing with her mobile device.

3. Alice activates the photo application on her device and selects a picture to print.

4. Alice taps her mobile device to the printer to initiate connection of the two devices.

5. If this is the first time, Alice confirms her trust in the connection with this printer.

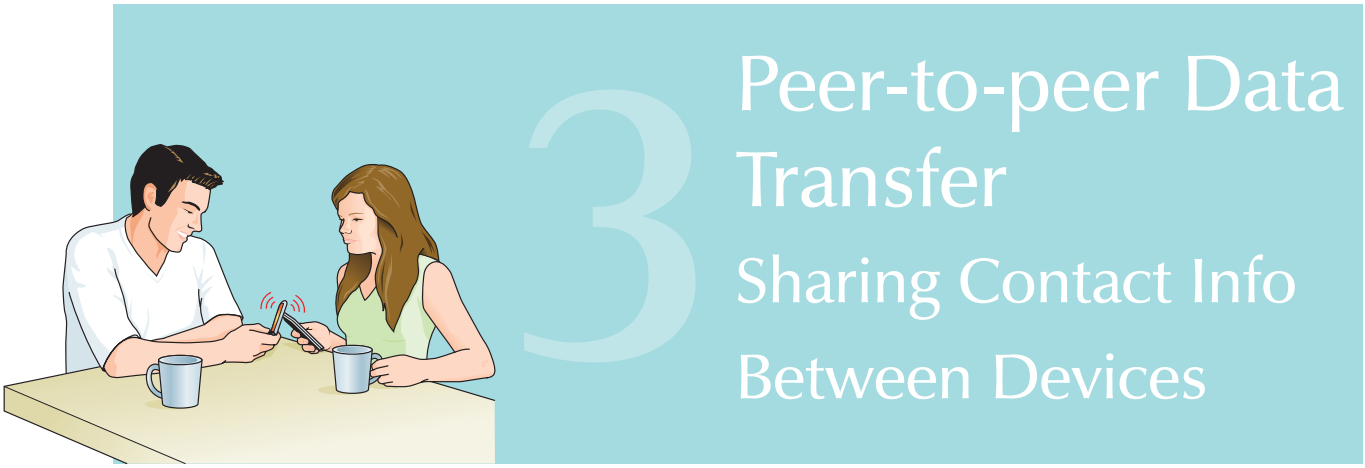
6. In the future, Alice can simply tap and print.

7. Once both devices are connected, the picture will be received and printed on the printer.

IPR2025-01151
Apple EX1039 Page 10

Key threats for users

- RISK 1: Original passive NFC tags can be modified to relay and divert the Bluetooth connection to a nearby malicious device that will surreptitiously connect to Alice's mobile device and either store or print Alice's picture, rather than connecting to the intended printer.
- RISK 2: Original passive NFC tag can be replaced by a malicious tag with similar intentions as Risk 1.



The Peer-to-peer data transfer use case enables the peer-to-peer mode to provide a simple way to share data between two NFC devices over an alternative communications carrier. Similar scenarios include sharing videos, links, business cards and personal contact information; synchronizing phones and playing multiplayer games.

Actors in the use case scenario #3

- Peter, who wants to share a contact.
- Alice, who wants to receive the contact.
- Address book with Bluetooth transfer capability.
- Mobile device with NFC content-sharing capability.

Description of events

1. At a conference, Alice meets Peter for the first time and Peter, using their mobile devices, wants to share an address book contact with Alice over a Bluetooth connection.

IPR2025-01151
Apple EX1039 Page 11

2. Peter knows that NFC is available on both their devices to facilitate rapid sharing of content over a Bluetooth connection.

3. Peter unlocks his smartphone, opens his address book and selects the contact he wants to share.

4. Alice unlocks her smartphone and waits for Peter to initiate the NFC interaction.

5. Peter taps Alice's phone to begin the NFC initiation of limited content sharing between their devices.

6. Alice is prompted by her smartphone to receive a Bluetooth connection with Peter's phone.

7. Alice confirms, and the Bluetooth connection with Peter's smartphone is created and the contact is transferred to Alice's mobile device.

Key threats for users

- RISK 1: With the close proximity of devices, eavesdropping, while difficult, is not impossible, without being detected by the legitimate owner of the devices.
- RISK 2: Sender shares malicious content instead of innocent content promised to receiver.
- RISK 3: As with all sharing of any content, sender does not have any control over subsequent sharing of their content by receiver.
- RISK 4: User may not be aware of which mobile application is the default handler for received content shared over a communication carrier initiated by an NFC-sharing interaction. This could lead to unforeseen storage or processing of the content.

IPR2025-01151
Apple EX1039 Page 12

4 Secure NFC Card

Presenting a Loyalty "Card"

The Secure NFC Card use case enables both the card emulation mode and on-device hardware security elements to provide a secure, contactless smart card for transactions such as access, payment or loyalty program. Similar scenarios include: presenting secure NFC card credentials that represent or authenticate individuals' identities; providing access to physical workplace facilities, sporting events, theme parks, transit systems, and other restricted-flow areas; and for making financial payments.

Actors in the use case scenario #4

- Peter, who wants to collect loyalty points for a purchase at a game store.
- Game store, which creates customer repeat business with an in-store loyalty program.
- Secure NFC card point-of-sale system.
- Game store loyalty service.
- Mobile device with Secure NFC card capability.

Description of events

1. As Peter completes a game purchase at his local game store he is prompted by the point-of-sale system for his game store loyalty card credentials. In the past, this was provided on a swipe or smartcard.

2. Peter knows that he can use the Secure NFC card capability on his smart phone as an alternative to carrying his game store loyalty smart card in his wallet.

3. Peter has previously added his game store loyalty credentials to his Secure NFC card capability via his smartphone.

4. Peter unlocks his smartphone, then taps the phone to the point-of-sale device when prompted to provide his loyalty program credentials.

IPR2025-01151
Apple EX1039 Page 13

5. The point-of-sale system interacts with the game store loyalty service to register the sale and return the associated loyalty point value, which it writes to the Secure NFC store on Peter's smartphone.

6. Peter gets a prompt from the Secure NFC card point-of-sale device that 500 points have been added to his loyalty card account.

Key threats for users

- RISK 1: Even with the close proximity of devices, eavesdropping security risk is possible, without detection by the legitimate owners of the devices.
- RISK 2: The game store loyalty program could be used to profile Peter's purchasing habits, deploy that profile information for targeted advertising and shared with third-parties, without Peter's knowledge and consent.
- RISK 3: The game store loyalty program could be the target of a data breach which could cause Peter to be the victim of identity theft (depending on the data that the loyalty system collects and retains about their members).

Applying *Privacy by Design* to Mitigate Risks

NFC ecosystem players can look to the 7 Foundational Principles of *Privacy by Design* for approaches to mitigate the risks identified in the NFC use cases. NFC ecosystem players include the NFC Forum, NFC device manufacturers, NFC application developers, businesses developing NFC service use cases such as smart posters, mobile operators and individual users. In addition, the NFC ecosystem interacts with existing Internet and Web ecosystems and so should coordinate its security and privacy strategy with these other ecosystem stakeholders.

1. ***Proactive*** not Reactive; ***Preventative*** not Remedial

- NFC device manufacturer: NFC capability is designed with a prominent prompt framework that consistently cues users to impending interactions.
- NFC application developer: Mitigate against threats such as malicious tag modification or replacement by designing in "tag filtering". For example, if your NFC application implements a smart poster reader application that is designed to only support mobile browser access to online information (e.g., expects only to see a HTTP URL tag type), then the application should provide robust tag reading capability that filters out all out-of-scope tag types, such as an SMS messaging URL or a FILE URL tag type. A malicious SMS messaging URL tag can introduce unwanted inbox messages that can be inadvertently opened and acted on by the user, or can be used to send unwanted premium SMS messages, causing unauthorized consumer charges. A malicious FILE URL can be used to invoke

IPR2025-01151
Apple EX1039 Page 14

a Trojan file previously installed on the mobile device. SMS and FILE URL NFC requests should always include NFC application implementation of strong tag type filtering and explicit user confirmation prior to invocation.

- NFC application developer: System and application bugs and design issues are leading causes for existing security and privacy vulnerabilities in ICT systems. NFC application developers should include security and privacy impact assessments as part of their quality control processes, in which system and application code can be reviewed for possible threat vulnerabilities, as well as for potential design improvements, to mitigate such risks.

2. Privacy as the *Default Setting*

- NFC application developer: Automatically turn off the alternative communication carrier (e.g., Bluetooth connection) upon completion of the user-initiated actions or interaction. For example, after transferring a photo over a Bluetooth connection from one NFC-enabled mobile device to another, the NFC applications on both devices should shut down the connection and if the Bluetooth radio was disabled prior to the content transfer, then also disable the Bluetooth radio.
- NFC device manufacturer: NFC capability should be disabled when the screen or keyboard of the mobile device is locked (e.g., screen is dark). NFC capability should only be active when the device is active for consumer use.

3. Privacy *Embedded* into Design

- NFC device manufacturer: Provide a platform connectivity setting that allows the user to disable his or her NFC capabilities.
- NFC application developer: NFC applications should respect the platform connectivity settings (e.g., NFC, Bluetooth, WiFi, Data radios) and alert the consumer in the event that needed connectivity for the application use case is disabled, because the application may not be able to work as intended.
- The NFC application developer: Instead of automatically triggering the NFC interaction specified in an NFC tag, the NFC application on the recipient device should prompt the user with information concerning the type of interaction (e.g., launch a browser, make a call, send a text message) and detailed interaction data (e.g., HTTP URL, international formatted phone number, phone number and SMS text). In addition, the application should seek user confirmation prior to proceeding with the interaction.
- NFC device manufacturer: Most of the NFC use cases involve launching an alternative communications carrier such as a mobile data service, Bluetooth or WiFi radio connections. Proper design should include adequate prompting users with information to help understand the pending interaction and impact to the users' privacy. The alternative communication carriers may have built-in

IPR2025-01151
Apple EX1039 Page 15

user prompts associated with connection setup that may not provide sufficient information about the interaction. For example, NFC application may assume that the Bluetooth subsystem will provide prompts for data transfers, but it may not provide adequate feedback on the type, name, or size of data about to be received. NFC device manufacturers need to consider the holistic, platform-wide solution being provided and the privacy design aspects that each component element in their design adds to the overall solution, to avoid false assumption that privacy will be handled by some other component within their solution (e.g., NFC data transfer application assuming Bluetooth stack on the mobile device will inform the user of details of the data to be received).

4. Full Functionality — ***Positive-Sum***, not Zero-Sum

- NFC application developer: A data governance policy should be defined that clarifies what personal data is being collected and its intended purpose, by the service launching the smart poster tag. The data governance policy should also define the data retention details for any collected data, what entities are acting as data controller and data processor for the data and whether the data will be transferred across national boundaries to fulfill the primary purposes of the service associated with the smart poster.

5. End-to-end Security — ***Full Lifecycle Protection***

- NFC device manufacturer: When implementing peer-to-peer use case support, device identity should be regenerated on each interaction with a random identifier not tied to persistent, device-unique identification such as the telecommunications device unique identifier.
- NFC application developer: When creating applications, especially within the peer-to-peer category, NFC application developers should also be cautious about design elements that create a persistent linkage of the NFC usage to the user or individual mobile device (e.g., MSISDN, IMEI, gamer player identifier "XYZ", etc.). Collection of personal information such as a unique device identifier should be featured in the notification provided to users.

6. ***Visibility*** and ***Transparency*** — Keep it ***Open***

- NFC application developer: Do not consider using covert or hidden NFC tags that permit consumer tracking for non-security reasons. Keep your practices open and transparent to your users.

7. ***Respect*** for User Privacy — Keep it ***User-centric***

- Smart Poster developer: Provide a privacy notice on the smart poster that describes full and complete disclosure of what personal information will be collected/

IPR2025-01151
Apple EX1039 Page 16

processed/stored/transferred. Also provide contact information for users who want to have follow-up communication with the data controller of the service associated with the smart poster.

To be truly effective, *Privacy by Design* principles should be applied as early as possible in the development cycle and in the broadest scope, involving everyone in the ecosystem.

Residual Security and Privacy Risks

Despite many notable privacy by design features, several residual risks remain in the NFC technologies and ecosystem.

Automated Linkages to Other Communications Channels

NFC is used in a number of reference use cases to launch an alternative communication carrier, such as a mobile data connection to a website or to set up a WiFi hotspot connection. Secondary to setting up these connections, users will likely be accessing the Internet and Web. Security and privacy concerns already associated with such consumer online interactions apply in these cases, also. The value proposition for NFC is to provide an expedited connection setup to these alternative communication carriers. This means that NFC application developers might view user prompts, intended to caution users or remind them of pending interactions, as interfering with the primary NFC value proposition. *Privacy by Design* argues that both the business intent and the consumer privacy intent may be addressed in a win-win manner. However, this principle needs to be reinforced in the initial stages of product conception.

Inadequate User Information and Prompts

The "Tap 'n Go" NFC user experience facilitates quick service and data connections. But such ease of use can introduce security or privacy risks if the NFC request is an attack that is trying to create a data connection to a risky service, or to share unwanted or threatening content, or a Bluetooth pairing with an attacking entity. Such threats can lead to risks such as phishing for personal data from an attacking Internet site, or deploying unsolicited peer-to-peer malware that can lead to unwanted disclosure of personal data.

Typically, in each of the NFC use cases, the application should notify the recipient user of a pending NFC request (e.g., initiate a service, start a Bluetooth pairing or share a file). Additionally, the user should be given the opportunity to confirm the request (e.g., "Do you really want to accept the file?"), providing the user with two steps to initiating a NFC request. Due to possible abuse of data in NFC tags by attackers, NFC application developers should also take design steps to ensure that their applications correctly display the prompts contained in the data within tags. For example, attackers can insert reversing, non-spacing

IPR2025-01151
Apple EX1039 Page 17

or control characters into prompt text within a NFC tag to deceive a user into confirming a NFC request. By designing an application to assert filtering of tag data to remove unexpected characters, the application can limit the harm of such attacks.

Poor Application Design

NFC is targeting implementation in personal devices (mobile phones, their accessories, etc.) so it is a plausible scenario that there could be applications that also transfer and process personal data. This may give rise to "privacy breach" or "data leak" types of privacy risks. This risk is common with almost any mobile application and service, and similar controls should be employed: Applications should apply data minimization when sending data, and should use appropriate security mechanisms to harden the data both on device and in transit. Mobile platforms, in turn, should have a way to manage the application's (NFC or other type of apps) access to personal information.

The threats to NFC applications are primarily related to information security. However, these threats present the risk of misuse of consumer data, creating privacy threats.

Interoperability Vulnerabilities in Hardware and Platforms

A general threat to NFC applications can manifest itself through possible vulnerabilities in the underlying NFC enabler on the mobile device, for example, the exploit of weaknesses in the NFC device driver in the operating system of the mobile device. Currently-deployed mobile devices supporting NFC run on differing mobile device operating systems, making analysis of such risks difficult. NFC application developers should consult with NFC industry security and privacy experts to determine whether their target mobile device platforms have known security or privacy vulnerabilities and possible corrections.

Tampering and Spoofing of NFC Tags

The UID element in NFC tags has the potential threat of tampering and spoofing. The typical mitigation of this threat is to provide a tamper-resistant "seal" and to sign the object with a credential from a trusted authority, thus providing a reference of authenticity for recipient entities. The NFC Forum specifications include a framework for signing multiple NFC data exchange format records (NDEF) in NFC tags, to help assure that the originator of the tag and its information are trusted. However, NFC ecosystem participants might additionally consider agreeing on a set of reference certificate authorities (e.g. providers of root certificates) and also adding the signature framework to their NFC interoperability certification for use in future products and services.

Additionally, NFC standards should be periodically reviewed with the intent of new work items to supplement the stack of specifications with additional standards or implementation

IPR2025-01151
Apple EX1039 Page 18

profiles to address identified gaps in the current version of these standards. For example, as noted above, current NFC standards do not completely provide a common approach to ensuring the authenticity to NFC tag data. For example, a digital signing approach could be standardized to help ensure that the originator of the tag and its information is trusted and not tampered with.

Corrupted or Malicious Tag Data

Side effects to consumers from abuse of NFC tags could lead to one of the most serious security and privacy threats to NFC application developers. Consumer trust in the NFC ecosystem could be eroded by misleading the consumer with corrupted tag data, leading to serious economic impacts to both consumers and business alike. Since tags are generally physically idle and are technically passive, they can become a target of attack. NFC tags could be cloned with corrupt tag data that would either include an unwanted request or mislead a user into confirming the NFC request. Providers of services that utilize publicly-located NFC tags should develop physical security and privacy controls that help mitigate this risk.

Emerging Environments, Infrastructures of Ubiquitous Surveillance

NFC is compatible with certain passive RFID tags. The growing presence of RFID tags in physical environments should be addressed, because they have their own respective privacy implications. In particular, having NFC on mobile devices may mean that RFID readers become widespread and any security or privacy aspects of ubiquitous RFID tags may have to be reassessed. In particular, legacy RFID tag-based systems should begin to assume that the tags can be easily read by anyone with a mobile NFC-enabled device, so proper security controls should be based on a tag being hard to read (or, in some cases, hard to rewrite).

As NFC technologies become more ubiquitous, developers might create concepts that involve installing NFC readers on laptops or other network-connected personal devices, as well as creating personal identification accessories with passive NFC tags. These two developments present the potential for the physical behaviour of a user being tracked and the inherent privacy risks of hidden data bases containing such profile information.

These residual risks may be mitigated somewhat by effective notice requirements, such as the prominent presence of the recognized NFC mark (shown at left) to indicate the presence of a tag and reader. However, in some cases, a more comprehensive *Privacy by Design* risk-based approach is warranted.

IPR2025-01151
Apple EX1039 Page 19

Conclusions

- The design and deployment of NFC technology offers new conveniences and benefits to users, and represents several advances in security and privacy over traditional architectures.
- Ensuring that security and effective user privacy defaults and controls are built into NFC applications is critical to assuring widespread trust, adoption and innovation of this technology.
- Not all privacy and security concerns may be addressed solely by the NFC technology and standards – the broader NFC ecosystem must be aligned with the security and privacy benefits. This will require co-operation on the part of all NFC ecosystem players, notably application developers.
- *Privacy by Design* principles are instrumental in helping to achieve this cooperation and alignment.
- Nokia is a leading global player in the NFC ecosystem and is working to ensure that *Privacy by Design* principles are embedded in their products and services, including NFC technologies.

IPR2025-01151
Apple EX1039 Page 20

References

NFC Forum: www.nfc-forum.org

NFC World: www.nfcworld.com

NFC Nokia: http://europe.nokia.com/nfc

Office of the Information and Privacy Commissioner (IPC) of Ontario, Canada: www.ipc.on.ca

Privacy by Design (*PbD*): www.PrivacybyDesign.ca

Chris Foresman, "Near Field Communications: a technology primer," *Ars Technica* (February 2011), at: http://arstechnica.com/gadgets/guides/2011/02/near-field-communications-a-technology-primer.ars

B. Joan, (n.d.). "Difference Between RFID and NFC," *Difference Between*. Retrieved September 26, 2011, at www.differencebetween.net/technology/difference-between-rfid-and-nfc/

Harley Geiger, Center for Democracy and Trust, *NFC Phones Raise Opportunities, Privacy And Security Issues* (April 2011), at: www.cdt.org/blogs/harley-geiger/nfc-phones-raise-opportunities-privacy-and-security-issues

Collin Mulliner,

— "Attacking NFC Mobile Phones," 2008. at: www.mulliner.org/nfc/feed/collin_mulliner_eusecwest08_attacking_nfc_phones.pdf

— "Vulnerability Analysis and Attacks on NFC-enabled Mobile Phones," International Conference on Availability, Reliability and Security, IEEE Computer Society, 2009, at www.mulliner.org/collin/academic/publications/vulnanalysisattacksnfcmobilephones_mulliner_2009.pdf

Christian Kantner, Josef Langer, Gerald Madlmayr, Josef Scharinger, "NFC Devices: Security and Privacy," The Third International Conference on Availability, Reliability and Security, IEEE Computer Society, 2008, at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&tarnumber=4529403

Dr. Marnix Dekker and Dr. Giles Hogben, European Network and Information Security Agency (ENISA),

— *Appstore security: 5 lines of defence against malware* (September 2011), at: www.enisa.europa.eu/act/application-security/smartphone-security-1/appstore-security-5-lines-of-defence-against-malware

— *Smartphones: Information security risks, opportunities and recommendations for users* (December 2010), at: www.enisa.europa.eu/act/it/oar/smartphones-information-security-risks-opportunities-and-recommendations-for-users

— *Top Ten Smart Phone Risks*: at www.enisa.europa.eu/act/application-security/smartphone-security-1/top-ten-risks

IPR2025-01151
Apple EX1039 Page 21

Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario
Canada M4W 1A8
Telephone: (416) 326-3333
Fax: (416) 325-9195
E-mail: info@ipc.on.ca
Website: www.ipc.on.ca

November 2011

Privacy by Design: www.privacybydesign.ca

Information and Privacy Commissioner,
Ontario, Canada