On-demand RFID: Improving Privacy, Security, and User Trust in RFID Activation through Physically-Intuitive Design

Youngwook Do*†[1], Tingyu Cheng†§, Yuxi Wu†¶, HyunJoo Oh†‡, Daniel J. Wilson‖**, Gregory D. Abowd††, Sauvik Das‡‡
*Global Technology Applied Research, JPMorganChase
†School of Interactive Computing, Georgia Institute of Technology
‡School of Industrial Design, Georgia Institute of Technology
§Department of Computer Science and Engineering, Unversity of Notre Dame
¶Khoury College of Computer Sciences, Northeastern University
‖Kostas Research Institute, Northeastern University
**Department of Chemical Engineering, Northeastern University
††Department of Electrical and Computer Engineering, Northeastern University
‡‡Human-Computer Interaction Institute, Carnegie Mellon University
Emails: youngwook.do@jpmchase.com, tcheng2@nd.edu, yux.wu@northeastern.edu, hyunjoo.oh@gatech.edu, da.wilson@northeastern.edu, g.abowd@northeastern.edu, sauvik@cmu.edu

***Abstract*—Passive RFID is ubiquitous for key use-cases that include authentication, contactless payment, and location tracking. Yet, RFID chips can be read without users' knowledge and consent, causing security and privacy concerns that reduce trust. To improve trust, we employed physically-intuitive design principles to create On-demand RFID (ORFID). ORFID's antenna, disconnected by default, can only be re-connected by a user pressing and holding the tag. When the user lets go, the antenna automatically disconnects. ORFID helps users visibly examine the antenna's connection: by pressing a liquid well, users can observe themselves pushing out a dyed, conductive liquid to fill the void between the antenna's two bisected ends; by releasing their hold, they can see the liquid recede. A controlled evaluation with 17 participants showed that users trusted ORFID significantly more than a commodity RFID tag, both with and without an RFID-blocking wallet. Users attributed this increased trust to visible state inspection and intentional activation.**

I. Introduction

Seamlessness is a long-vaunted design goal for ubiquitous sensing systems [1], but begets significant security and privacy (S&P) concerns that can reduce user trust [2]. Radio-frequency ID (RFID) chips exemplify this seamlessness in that they are battery-free, can be hidden within ordinary objects like cards, and enable a rich tapestry of simple interactions such as keyless authentication into physical spaces and cars, contactless payments, and indoor position tracking [3]. And yet, the ACLU warns, this same technology "has the potential to jeopardize consumer privacy, reduce or eliminate purchasing anonymity, and threaten civil liberties" by making it possible "for governments, stores, and hackers to identify people at a distance and without their knowledge." [4] Similarly, in a document published by the U.S. Department of State regarding use of U.S. Passport Cards, it was reported that four Members of Congress, as well as technology, security, and privacy groups, expressed concern that unauthorized entities could surreptitiously capture data in the RFID-chip embedded in passport card [5].

In an effort to respond to such concerns, recent work has shown the promise of tangible and 'physically-intuitive' design that employs end-users' understanding of the real world physics. For example, automated physical barriers that block webcams when not in use increase trust by providing users with perceptible assurance that they cannot be seen when they do not want to be seen [6]. Microphones that can only be powered through intentional interaction convince people that they cannot be heard when they do not want to be heard [7]. The theory is that tangibility and physical-intuition in privacy controls can bridge the gap between how users *believe* a control works and how it *actually* works [8]. In this paper, we ask: *how can we employ physically-intuitive design principles to build an RFID chip that users trust can only be activated when they want it to be activated?*

There is already evidence of a sizable need and desire for physically-intuitive S&P controls for RFID chips. Today, users with strong S&P concerns over RFID technology turn to using metal-lined wallet sleeves. Similarly, U.S. passport cards get issued with a card sleeve to prevent unauthorized access [5].

[1]This research was conducted prior to joining JPMorganChase

Symposium on Usable Security and Privacy (USEC) 2025
24 February 2025, San Diego, CA, USA
ISBN 979-8-9919276-5-9
https://dx.doi.org/10.14722/usec.2025.23006
www.ndss-symposium.org, https://www.usablesecurity.net/USEC/

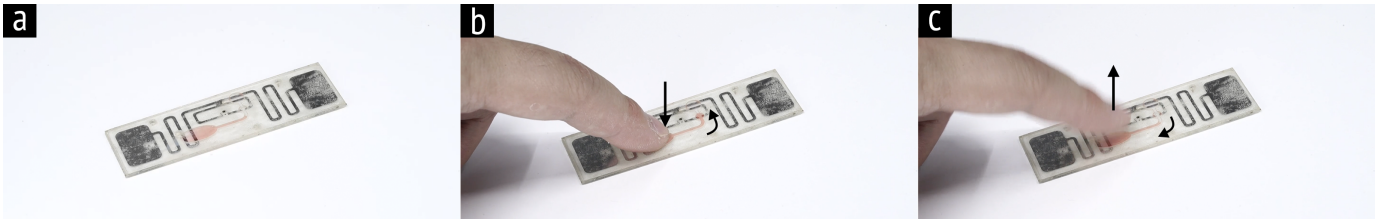

Fig. 1. Commodity RFID chips allow for passive data emission, raising security and privacy concerns because data can be read without users' knowledge and consent. To improve trust, On-demand RFID aligns RFID activation with user intention, allowing users to only intentionally activate the RFID chip and visibly inspect its state. (a) By default, the RFID antenna is disconnected, disabling data emission. (b) To activate On-Demand RFID, a user can press its inkwell to push the conductive liquid to a reservoir that bridges the bisected antenna, enabling data emission. (c) To deactivate On-demand RFID, users need only release their finger, which causes the conductive liquid to retract back into the inkwell, disconnecting the antenna once more.

But this is a band-aid solution that puts the onus on users to actively procure extra protection, and has been shown to not fully block emitted RF signals [9] — imposing both a usability burden without fully mitigating the S&P risk. To improve on the state-of-the-art, we designed and developed On-demand RFID, a passive RFID chip that employs physically-intuitive design principles.

With On-demand RFID, the antenna that emits the information stored in the tag is disconnected by default, disabling the passive and non-consensual reads that underlie the surveillance and security concerns described above. To re-connect the antenna, users must complete the circuit by pressing down on a chamber that contains visible conductive ink. Doing so pushes the conductive ink, through a fabricated microfluidic channel, towards a reservoir that bisects the antenna, completing the circuit and allowing for data emission (see Figure 1). Additionally, by using a "dead-man's switch" design, the antenna is automatically disconnected when On-demand RFID is not in use, eliminating the need for users to remember to disconnect the antenna. When the user releases their finger, the ink automatically recedes back to the original chamber. This approach takes inspiration from the techniques introduced by Sun et al. [10], who first explored the use of microfluidics in RFID.

On-demand RFID embodies physically-intuitive design principles in two ways. Prior work suggests one way to improve trust through physically-intuitive design is through perceptible assurance of sensor state [7], [8]. To that end, in On-demand RFID, the conductive ink is visible to users at all times so that the state of the antenna connection is always clear, providing users with perceptible assurance as to whether their tag can be sensed or not. Prior work also suggests that manual activation and automatic deactivation engender trust [6]. To that end, On-demand RFID requires intentional, manual activation from users but is automatically deactivated when that active engagement ends. This requirement of continuous manual activation creates a reflexive and intuitive link between action and state, preventing unwanted and non-consensual reads. Beyond these key changes, a secondary design goal was to otherwise keep the form factor of RFID chips as close to the same as possible: just as thin, and nearly as cheap.

Microfluidic-enabled RFID tags have been technically evaluated in the past [10]. We build on this prior work by evaluating *user trust* in this technology, through designing a high-fidelity technology probe [11] and conducting a within-subjects user study with 17 participants. We found that participants trusted that On-demand RFID could only be read in line with user intention significantly more than a commodity RFID tag both in and out of an RFID-blocking wallet, and that participants rated all three conditions as being highly usable. We further asked participants to explain their ratings during the study to better understand what underlined their trust and usability ratings. As hypothesized, participants described the need for intentional activation and the clear visual indication of state as key reasons for their increased trust in On-demand RFID. Participants also did discuss some concerns — e.g., the potential for accidental activation. Ultimately, our findings suggest that On-demand RFID increases trust without significantly impacting usability. Accordingly, for situations where people have significant S&P concerns (e.g., in payment contexts or for transmission of sensitive information like known traveler numbers), deploying solutions like On-demand RFID may be fruitful.

To summarize, in this paper, we present the following contributions: (1) Building on prior work on engendering trust in sensing systems through physically-intuitive design and microfluidics-enabled RFID, we designed and implemented an RFID tag that is activated on-demand to address S&P concerns with and users' trust in passive RFID technology; and, (2) we comparatively evaluated On-demand RFID to existing passive RFID chips both with and without RFID-blocking wallets, and found that it increases user trust relative to these baselines. Through an additional qualitative assessment, we found that users largely attributed this increased trust to the physically-intuitive design principles we followed. In short, our core contribution is the application and evaluation of a known technique to a novel use case [12]: i.e., improving user trust in RFID sensing systems.

II. Background and Prior Work

A. RFID Security and Privacy and Technical Solutions

Passive RFID technology has increasingly been embedded into our daily lives for numerous use cases (e.g., contactless payment, physical space access, car key, location tracking).

Its battery-free and wirelessly-power capabilities allow for nigh-seamless integration into physical spaces: users need not charge these devices, and can access their affordances through simple physical interactions (e.g., tapping a card against a reader). For these same reasons, passive RFID technology has also received a lot of attention, in the Human-Computer Interaction and Ubiquitous Computing communities, for battery-free wireless sensing of contextual information [13], [14], [15]. For example, prior work has explored various RF-based input and sensing techniques that leverage the impedance of a RF tag and/or resonant frequency changes affected by interactions with the tags [16], [17], [18], [19], [20], [21].

Despite those benefits, the widespread use of passive RFID technology has sparked and amplified conversations surrounding its S&P vulnerabilities. Passive RFID has been seamlessly deployed in everyday settings, which puts sensitive data stored in end-users' RFID tags at risk of being unwittingly scanned and monitored [22], [4], [23], [24], [25]. The primary factor behind this vulnerability is that data stored in a passive RFID is scannable and readable as long as *any* associated RFID reader is nearby [4] — with or without a user's knowledge and consent. In other words, users have no agency to prevent malicious actors from accessing the data stored in their passive RFID tags as long as the reader is within range. Moreover, recent research suggests that it is possible to create readers well beyond a user's line-of-sight. For instance, Wang et al. introduced a novel technique that enables a passive RFID tag to be readable from a distance of more than 50 meters [26].

One way people address the S&P problems of RFID today is by placing their RFID tags in metal sleeves or wallets. Metal can attenuate radio frequency signal transmissions [9], and can thus thwart attempts by adversaries to covertly read passive RFID signals from tags placed within the sleeve. Demands for these products are high enough that even Apple now produces an RFID-blocking physical wallet [27].

However, metal sleeves are not panaceas. Koscher et al. found that a metal sleeve may not fully block an RF transmission [9]. In this case, as RF transmissions are imperceptible, it would be challenging to discern whether RFID tags in the sleeve could stay readable. This finding implies that the metal sleeve that users think would work may not work as they expect, which creates a discrepancy in users' perception of how the protection functions [28]. In our work, we aim to design a novel protection method that guarantees their S&P in line with the users' perception and expectation of the protection.

B. Improving User Trust through Physically-Intuitive Design

The mismatch between how S&P operations work and how end-users think they work erodes trust in using sensor-enabled devices [28]. As a way to address this gulf, researchers have started adopting controls that are physically intuitive. By 'physically-intuitive' design, we mean designs that leverage end-users' knowledge of real-world physics to communicate how an S&P operation works. For example, people have an intuitive understanding that breaking line-of-sight with a camera can keep them out of a video recording. Relatedly, Ahmad et al. introduce the concept of 'tangible privacy' in which they discuss designing for tangibility as a way to narrow the gulf between the S&P actions users take and how they work [ibid].

In the webcam context, for example, many end-users employ physical barriers (e.g., tape, sticky note) to physically block their webcam to prevent covert webcam access [29]. Breaking line-of-sight is a physically intuitive idea that increases people's assurance that they cannot be "watched". Building on this practice, Do et al. introduced an intelligent physical barrier — Smart Webcam Cover — to automatically shield a laptop webcam once a user no longer uses a webcam, eliminating reliance on human memory for webcam covering [6]. They found that this intelligent automation improved users' trust in the effectiveness of the webcam cover. Similarly, Steil et al. demonstrate a physical cover that is mechanically actuated to block the camera of head-worn wearables [30]. Researchers also have studied perceptible solutions for microphone-enabled devices. For instance, smart speaker users used ad-hoc methods to address privacy concerns against unwitting recording by a smart speaker by staying away from, or by unplugging, the device [31], [32]. For example, NPR and Edison Research reported that more than 50% of the US population expressed their privacy concerns against 'always-listening' smart speaker microphones [33]. Ahmad et al. found that physical power disconnection of a microphone could physically guarantee that a microphone is disabled to record and, in turn, mitigate concerns about smart speakers [8]. Do et al. studied that a microphone's physical and visible power disconnection can engender more trust in using a smart speaker microphone than a smart speaker's built-in mute button [7]. Similarly, Chandrasekaran et al. found that powering off a smart speaker enhances trust in disabling microphone recording more than using a smart speaker's built-in mute feature [34].

Compared to microphone-enabled and camera-enabled devices, there have been few prior attempts to address end-user S&P concerns with passive RFID devices. Marquardt et al. introduce a technique that uses a mechanical switch to disconnect an RFID tag's antenna when a user does not want the tag to be detected [35]. Karjoth and Moskowitz illustrated techniques of severing an antenna from an RFID chip after the RFID usage [36]. However, whether a mechanical switch could address S&P concerns about RFID usage and build trust in using passive RFID technology was not studied. In our work, we introduce an intelligent and perceptible solution, building on prior work. Specifically, we designed the solution to automatically disable the passive RFID tag antenna when not in use for users to ensure that the RFID is readable only with a user's intention [6]. Additionally, RFID tag reading could be enabled and disabled by sensor-enabled switches [37], [35], [38] or by authentication via tactile communication between a mobile and an RFID tag [39]. Moreover, the RFID communication could be secured with software-based encryption [25]. However, our intention is to make the antenna

disconnection physical and visible to provide users perceptible assurance about the tag's RF signal transmission [7], [8]. Then, we evaluate if our method provides perceptible assurance about the deactivation of an RFID tag, compared to existing methods such as an RFID-blocking wallet.

III. On-demand RFID

Prior work suggests that the current passive RFID tag design entails S&P vulnerability where the tag information could be surreptitiously read and monitored without a user's knowledge or consent. Moreover, the tag could still remain readable even when a user puts the tag inside an RFID-blocking sleeve [9], which goes against users' expectations about the protection and could lead them to erode their trust in using the RFID protection method. To address this vulnerability and trust issue, we developed On-demand RFID. This section describes design considerations to develop On-demand RFID and how to implement it.

We note that the application of microfluidics to RFID tags itself is not novel [10]; nor are microfluidic-enabled RFID tags the only technology that meets the requirements for physically-intuitive design that we discuss in this section. Rather than evaluating On-demand RFID's technical feasibility or exploring alternative designs, our focus in this paper is to showcase the possibility of *designing* RFID chips that end-users can tangibly trust.

A. Design Considerations

1) RFID Antenna Disconnection to Disable RFID Read: There could be two ways to disallow an RFID tag to be read. One option is to power off the RFID reader, and the other is to disable the communication capability of an RFID tag. As our threat model is a situation where a user is unaware of when and from where their tags are being monitored or read, our target situation excludes the case where a user can access the reader to shut it off. To that end, our design focus is to make an RFID tag unable to communicate its stored data. Researchers have studied an RFID's antenna disconnection to disable the RFID tag reading when intended [10], [35], [40], [41], [42]. Since disconnecting power is a proven method to amplify user trust, for instance, in using a microphone [7], [8], we adopted a similar approach for RFIDs. Specifically, once the RFID antenna was physically disconnected, the RFID chip could not be powered and, in turn, could not transmit the data stored in the chip back to the RFID reader.

2) Perceptible Operation: For end-users to ensure their S&P control, prior work emphasizes the importance of providing perceptible assurance about their S&P operations, which helps them to understand and improves trust in how their control can protect themselves from a threat model [6], [7], [8]. For example, while a pressure-sensitive button demonstrated by Marquardt et al. enables an RFID tag antenna's physical connection and disconnection, the connection and disconnection are not visible to users [35]. To that end, one of the key insights for designing On-demand RFID is to create a method that allows end-users to perceptibly ensure their S&P control. For our design, we designed On-demand RFID to provide a clear indication of the antenna disconnection when a user has no intention to use an RFID tag and the antenna connection only when in use. To do so, we leveraged physical and tangible operations to enable direct manipulation [43].

3) Manual Activation and Automated Deactivation: People often forget to follow secure cybersecurity practices. Do et al. found that having agency over sensor usage with manual control while automating the deactivation of sensor usage improves trust in using the sensor [6]. Automating the deactivation of sensor usage eliminates reliance on human memory to remember to follow a secure practice and manual control to activate the sensor disallows others than a user to activate the sensor without the user's knowledge [ibid]. This way, sensor usage can be aligned with users' intentions, which in turn engenders trust in using sensors. Inspired by the combination of manual activation and automated deactivation, we took into account designing On-demand RFID for a passive RFID to be activated on demand.

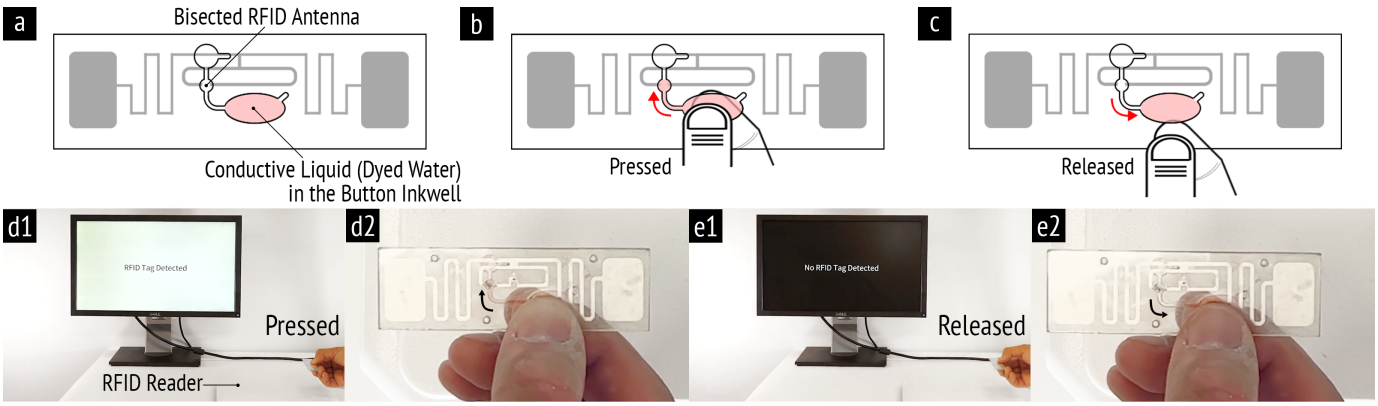

Fig. 2. On-demand RFID leverages the disconnection and connection of an RFID antenna to disable and enable the RFID tag reading, respectively. (a) By default, the antenna of On-demand RFID is severed in the middle. (b, d1, d2) Once a user presses a chamber of the microfluidic channel of On-demand RFID, the conductive liquid stored in the chamber is pushed to bridge the severed antenna trace, which enables the RFID tag reading. (c, e1, e2) Once a user releases their finger touch, the liquid goes back to the chamber automatically, which disconnects the antenna trace again and disables data emission.

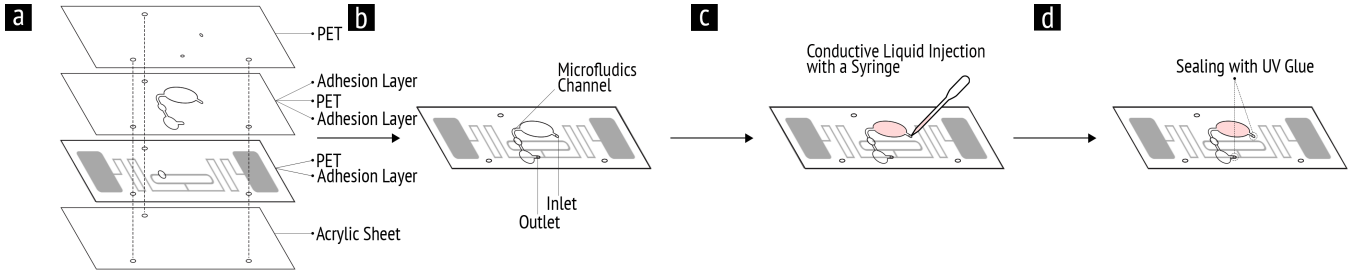

Fig. 3. On-demand RFID fabrication process. (a-b) On-demand RFID consists of a 4-layer structure. Each layer is stuck to the other by attaching an adhesive layer in between. We made three reference holes to align all the layer stacking correctly. (c) Then, we injected dyed conductive liquid (water) into the microfluidic channel through the inlet of the outer layer. (d) Once the injection is completed, the inlet and outlet are sealed by a UV-curing glue.

4) Simple Interaction and Form Factor: A key benefit of RFID technology is that it has an unobtrusive form factor and requires little direct user interaction. However, typical users often do not prioritize S&P for their everyday interactions [44]. For example, even if a mechanical switch could enable physical connection and disconnection of an RFID tag's antenna [35], it could be too bulky to be practical to achieve the thin card form factor of RFID use cases such as contactless payment and enhanced driver license. Additionally, the RFID antenna could be severed to allow a user to touch two metal contacts with a finger to bridge the antenna circuit [ibid] though users need to remove their gloves if wearing gloves without conductive tips. To that end, they would likely give up following a secured practice if it is cumbersome to use. Thus, security improvements must be balanced against usability encumbrances. Accordingly, we strove to keep the form factor and interaction affordances of On-demand RFID as close to that of a conventional RFID tag as possible.

B. Implementation

1) Microfluidics for On-demand RFID: In pursuit of a design that prioritizes intuitive physical interactions, fostering user trust, we employed microfluidics as the actuation mechanism for On-demand RFID. Microfluidics is a technology that harnesses the controlled movement of fluids within narrow channels to enable a wide range of computational functions, including sensing, actuation, and visualization [45], [10], [46], [47]. We determined that microfluidics technology aligns with all the design considerations we have previously discussed. Our initial goal was to establish a physically intuitive antenna connection and disconnection process, which we achieved by utilizing the movement of conductive liquid within the microfluidic channel. Specifically, our design defaults to a disconnected antenna state (see Figure 2 (a)), which becomes connected when conductive liquid bridges the antenna trace upon user activation. To facilitate this, users simply press a microfluidic button, causing the liquid to bridge the bisected antenna (see Figure 2 (b, d1, d2)). Since our device's fluidic system is sealed, releasing the button triggers fluid retraction, returning the antenna to its original disconnected state (see Figure 2 (c, e1, e2)). Furthermore, we dyed the liquid with red ink to provide visibility for the antenna's connection and disconnection. In the following subsection, we will describe our design's structure.

2) Structure:

a) Layers: Following and modifying the technique demonstrated by Wilson et al., we used a 4-layer structure to fabricate On-demand RFID (see Figure 3) [48]. The first layer consists of an acrylic sheet serving as the rigid substrate. On top of the first layer, we overlaid an RFID tag using common alignment holes and a custom-fabricated pin alignment tool. For the RFID tag, we used an off-the-shelf UHF RFID tag and its antenna was intentionally broken by cutting to enable reversible activation of the device using microfluidic features. We chose a UHF RFID tag for our proof-of-concept for two reasons. First, these tags are currently deployed in our target use-cases — such as an enhanced driver's license (EDL) [9] — where users carry the tags around and must hold them out for use. For example, to use their EDL in border crossing situations, a user must hold their EDL facing towards a UHF reader [49]. Second, we found that the commodity UHF tag's antenna traces, in general, have wider spacing than a standard HF tag's antenna traces, making it easier to fabricate a cut in the middle of the antenna trace. Next, we stacked a PET sheet featuring the microfluidic channel, which we fabricated using a CO2 laser cutter, onto the RFID tag. Lastly, we used another layer of PET to seal the microfluidic channel. Between layers, we attached pressure-sensitive adhesive sheets to bond the device together. After stacking and attaching the layers, we used a laminator to seal the microfluidic channel.

b) Channel Design: As illustrated in Figure 3 (b), we designed and implemented the microfluidic channel. The key concept behind the design is to enable the end-user to press a button chamber, facilitating the flow of conductive liquid through the carefully crafted microfluidic channel. The liquid is directed into a circular reservoir that intersects the RFID antenna trace. Through this process, the conductive liquid bridges the two open ends of the antenna trace which we cut off previously, thereby closing the circuit and activating the RFID tag for reading.

c) Conductive Liquid: When selecting the fluid for the microfluidic channels, we set two key criteria: (1) it needs to possess sufficient conductivity to restore the functionality of the RFID, and (2) it should offer a clear visual indication for

users to observe the circuit completion process. To meet these criteria, we used tap water as the conductive ink [10]. Then, we dyed it with red ink to make the liquid visible (see Figure 3 (c-d)). To inject the liquid, we created an inlet and an outlet on the top layer right next to the two chambers (see Figure 3 (b)). One chamber is to store the liquid to push to the bridge that connects the disconnected antenna. The other chamber is to keep air that is to push the liquid back to the original position once a user releases their finger press. We used a syringe to inject the liquid (see Figure 3 (c)). Once the button chamber was filled with liquid, we blocked the inlet and outlet holes by applying UV-cured glue (see Figure 3 (d)).

IV. User Study

We ran a user study to understand if and how applying physically-intuitive design principles to passive RFID tags — as manifested in On-demand RFID— affects end-user trust in using RFID technologies. We hypothesized that we would improve user trust in using a passive RFID tag compared to existing methods. Moreover, by reducing the difference in form factor and interaction affordance between On-demand RFID and a standard RFID tag, we hypothesized that while users may consider On-demand RFID less usable than a standard RFID tag, this perceived usability difference would be minimal. To test our hypotheses, we ran an in-lab, within-subjects, controlled experiment comparing On-demand RFID, along the dimensions of trust and usability, to two baselines: (i) a commodity passive RFID tag intact, and (ii) a commodity passive RFID tag inside an RFID-blocking wallet.

A. Threat Model

In this work, we are specifically interested in countering the threat of adversaries who can place RFID readers physically near users and try to covertly read the data stored in a user's passive RFID tag through these readers. Adversaries who can physically access and manipulate users' RFID tags are out of scope.

B. Method

1) Recruitment: We promoted our study by attaching flyers around our institution, sending emails to institutional mailing lists, and sharing information about the study on social media platforms (e.g., Reddit, Slack, Kakao, Instagram, Microsoft Teams). We made a concerted effort to recruit a balanced group of participants, roughly half of whom expressed privacy concerns with RFID technologies or other sensing systems and the rest of whom expressed little to no such concern. We used a pre-screener via email to recruit each group of participants. We recruited participants across demographic factors such as gender, age, and technical background based on their education and career in computer science or related fields.

2) Study Setup: Our study consisted of two phases: (1) evaluating the usability of each condition, and (2) assessing how much users' trusted that a malicious reader could not read the RFID tag they were given for each condition.

TABLE I
Demographics of the user study participants

Gender		Age		CS Education		CS Career	
Male	8	18-24	5	CS	12	CS	8
Female	8	25-34	11	Non-CS	5	Non-CS	9
Non-binary	1	35-44	-				
		45-54	-				
		55-64	1				

We used an ultra-high-frequency (UHF) RF reader and a UHF RFID tag in our study. Specifically, we used an ImpinJ Speedway R420 RFID reader, along with a Laird S9028PCR antenna that covers radio frequencies between 902MHz and 958MHz. We used Octane SDK to create a system that reads a UHF RFID tag and provides feedback accordingly.

During Phase 1, we placed the UFH RFID reader on a table, as well as a vault that could be opened and closed by placing the appropriate RFID tag on the reader. The purpose of the vault was to better simulate a practical security-relevant scenario for participants, such that they could reason about security risks, trust, and usability more concretely. To control the vault, we used a servo motor connected to an Arduino Uno board that received the digital signal triggered by an RFID reader. We also attached a handle to the servo motor's shaft to lock and unlock the vault.

To normalize distance-to-activation across conditions, we adjusted the sensitivity of the reader depending on whether participants were using On-demand RFID or a commodity RFID tag. On-demand RFID, in general, requires higher sensitivity settings on RFID readers; using these high-sensitivity settings for a commodity RFID tag would result in the tag being read from much longer distances than its standard. Accordingly, we set the transmission power stronger for On-demand RFID than the transmission power for a normal RFID.

In Phase 2, we placed a second RFID reader right next to the participant's seat. This reader was not connected to any RFID-reading system, but rather simulated potential malicious readers nearby with which users do not intend to interact. In the following subsection, we will further detail how all the setups were used during our study.

3) Procedure: We recruited 17 participants and conducted a within-subjects study with three conditions: **(A)** a commodity RFID tag in a non-RFID blocking wallet; **(B)** a commodity RFID tag in an RFID blocking wallet; and **(C)** an On-demand RFID tag in a non-RFID blocking wallet. We counterbalanced the order of these conditions with a Latin-square design.

Before Phase 1, we first asked participants if they had any S&P concerns with technology regarding data collection, monitoring, and tracking, including RFID technology, to confirm their responses from a prescreener. Also, we asked participants about their RFID use cases regularly to understand their RFID usage contexts. After probing their baseline RFID-related S&P concerns, we ran the study to compare the three aforementioned conditions (A, B, and C) in a counterbalanced order. We followed the same 2-phase procedure for each condition.

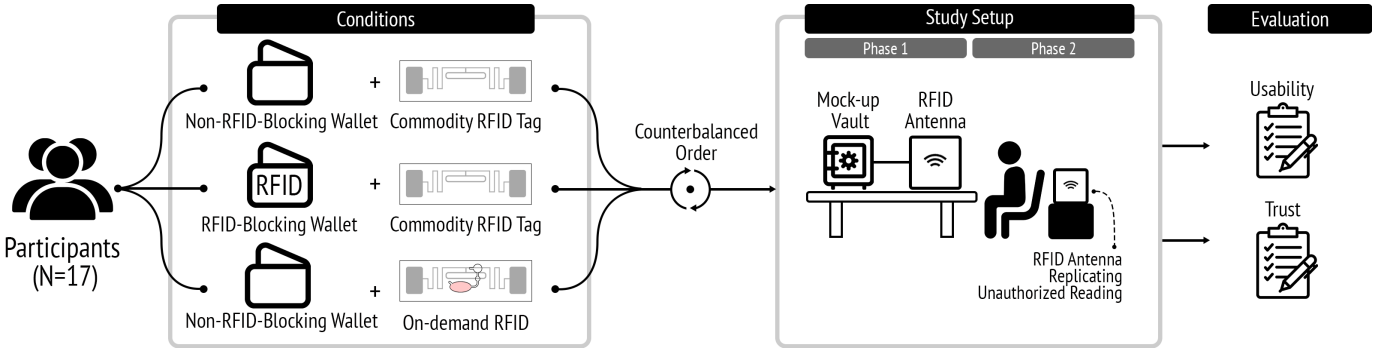

Fig. 4. We ran a user study to evaluate the usability of and trust in using On-demand RFID for passive RFID use cases, compared to existing RFID interactions. Participants were given three conditions: (i) a non-RFID-blocking wallet and a commodity RFID tag; (ii) an RFID-blocking wallet and a commodity RFID tag; and (iii) a non-RFID-blocking wallet and On-demand RFID.

In Phase 1, we first demonstrated interactions for successfully reading the RFID tag for a given condition. For example, during condition A, we demonstrated how to remove the tag from the non-RFID blocking wallet and tap the wallet directly on the reader; in condition B, how to remove the tag from the blocking-wallet and then tap it on the reader; and in condition C, how to remove the tag from the non-RFID blocking wallet and press down the ink-well on On-demand RFID and then tap it on the reader. For each condition, we showed participants how a user might use the RFID tag with a wallet. We also demonstrated how the blocking and non-blocking wallets can and cannot block the reader from reading the tag within the wallet, respectively. Then, we asked participants to put the wallet in their pocket, try to open and close the vault via the RFID tag interactions we demonstrated, and then put it back in their pocket when they were finished. If participants wanted to familiarize themselves further with the interactions and how each condition's tag and wallet worked, we encouraged them to repeat this process multiple times. After they were done, we asked participants to complete the system usability scale (SUS) form [50], which allows a participant to rate the usability of each condition quantitatively. Once they completed it, a researcher asked participants about their general reactions to each condition's interactions and follow-up questions according to their answers on the form. This way, we could understand participants' reasoning behind their SUS ratings.

In Phase 2, we wanted to understand participants' perceptions about the presence of an adversarial RFID reader. To do so, before the study started, we pre-placed a second RFID reader, not connected to the mock-up vault control, close to the chair where participants sat without telling them. This way, we replicated cases where users merely noticed the presence of RFID readers potentially used for covert scanning. At the beginning of Phase 2, a researcher informed participants that this RFID antenna had been situated close to the participant's pocket since the start of the study. Then, to measure trust, we asked participants to rate, on a Likert scale from 1 (Strongly disagree) – 5 (Strongly agree), to what extent they agreed with the following statement: "The tag is not readable when you don't intend to use the tag. (e.g., when putting it back in your pocket)". We refer to participants' answers to this prompt as the "trust score" below. Finally, we asked them about the reasons behind their trust score. We repeated this protocol for each condition.

We note that trust could be affected by various factors (e.g., competence, benevolence, integrity, predictability) [51], which could lead people to translate the definition of trust differently across different contexts. Despite the multi-faceted nature of trust, trust as it relates to the design of technical systems is often claimed to be associated with the property of meeting one's expectations [52], [53]. Taking inspiration from prior work, we specifically asked the aforementioned question instead of explicitly asking about trust in order to avoid any confusion from participants.

4) Hypotheses: We had two hypotheses.

- Participants will trust On-demand RFID more than commodity RFID tags, both when using and not using an RFID-blocking wallet.
- Participants will find On-demand RFID less usable than commodity RFID tags, both when using and not using an RFID-blocking wallet; however, the effect size of this usability decrease will be low.

We measured trust using the "trust score" described above. We measured usability using the System Usability Scale [50].

5) Ethics and Compensation: Our study design was approved by [Anon University]'s Institutional Review Board (IRB) before the recruitment. The study sessions took participants between 25-45 minutes. Participants received a 15 USD gift card as compensation upon their study completion.

6) Data Analysis: In our study, we analyzed both quantitative data and qualitative data. First, to evaluate our hypotheses, we comparatively analyzed two quantitative measures—the SUS evaluation and the trust rating—across the three conditions. Specifically, we used the Friedman test [54] and, as a posthoc test, the Wilcoxon-Signed Rank test [55], [56] to analyze the SUS and Likert scale rating results.

Next, we qualitatively analyzed their responses to our interview questions to better understand *why* participants expressed different levels of trust and/or usability across the three con-

ditions. Two researchers first transcribed the qualitative data of the user study. Then, we obtained codes from the data by running an open coding process and identified emergent themes by performing a thematic analysis based on the codes [57], [58]. Specifically, the first researcher extracted the codes by reviewing the qualitative data and created the codebook accordingly. The second researcher independently reviewed the codes following the transcribed data and iteratively updated the codebook as required. Lastly, the two researchers discussed the codes and the codebook. They continued to codify emergent themes by performing an axial coding process until reaching an agreement on the list of the themes [59]. Based on prior work [60], we did not use inter-rater reliability (IRR) measures, since the main purpose of our qualitative analysis was to understand emergent themes around trust in On-demand RFID, rather than to make generalizable claims.

C. Results

1) Quantitative Data Analysis: To test our hypotheses, we first employed a round of null hypothesis significance testing to assess if there were differences in trust and usability across the three conditions.

a) Trust: We hypothesized that participants would give On-demand RFID a higher trust-score than using a commodity RFID tag in both a blocking and non-blocking wallet. Our results confirm this hypothesis (see Figure 5). The median ratings for (Condition A) the non-RFID-blocking wallet and normal RFID tag, (Condition B) the RFID-blocking wallet and normal RFID tag, and (Condition C) the non-RFID-blocking wallet and On-demand RFID were 2, 4, and 5, respectively. To test if these differences across conditions were statistically significant, we performed a Friedman test and found a significant effect (χ^2=28.7, p$<$0.01). To identify statistically significant pairwise comparisons, we next ran a posthoc test with Wilcoxon Signed Rank test with Bonferroni correction and found statistical significance between all pairs among the three groups: (i) between Group A and B (p$<$0.01, r= 0.89); (ii) between Group B and C (p$<$0.05, r=0.78); and (iii) between Group C and A (p$<$0.01, r=0.88). In short, participants gave On-demand RFID a significantly higher trust score than both baselines, as hypothesized.

b) Usability: We hypothesized that participants would find On-demand RFID less usable because it requires active interaction where commodity RFID tags do not, but that the effect size of this usability difference would be small. We used the same tests we utilized in Section IV-C1b, but with the SUS scores for all three conditions. We did not find a significant difference between the three conditions (χ^2=4.48, p$>$0.05) based on the Friedman test results — p values are 0.495, 0.193, and 0.055 for pairs Group A-Group B, Group B-Group C, and Group C-Group A, respectively. These results suggest that we cannot reject the null hypothesis that there is no perceivable difference in usability across the three conditions. Looking closer, we observe that the median usability ratings were relatively high across all three conditions— 90, 87.5, and 82.5 for Group A, Group B, and Group C, respectively. Prior work suggests that any score above 80 is considered an "above average" experience [50] and has become an industry standard. While it is possible that we would have observed a significant relative effect in usability between On-demand RFID and the two baselines if we had more participants in our study, the absolute usability score for On-demand RFID is still above established standards for a good user experience.

2) Qualitative Data Analysis: We next report on our qualitative data to better understand what aspects of On-demand RFID improved user trust without significantly impacting usability. We found three key themes that affected participants' perceptions of trust and usability: (1) intentional activation, (2) perceptibility of state, and (3) physical practicality.

a) Intentional Activation Bolsters Trust, but Accidental Activation Erodes Trust: Many participants strongly believed that On-demand RFID would only be activated when they intended to use it. They appreciated that, through the need to actively press down on the inkwell, On-demand RFID afforded intentional activation. P11 mentioned that the "[On-demand RFID tag] would... align better with a user's intention." Likewise, when describing the reason to feel confident that On-demand RFID would only be activated when intended, P17 stated, "You need the effort to make it function, which means if you're not putting the effort...it will not work." In short, we found aligning RFID activation with a user's intention to press the inkwell helps enhance trust in passive RFID usage against malicious attempts to read RFID information unwittingly.

Concurrently, the possibility for *accidental* activation of On-demand RFID reduced trust for some participants. For example, participants worried that On-demand RFID could be accidentally activated when placed inside a tight wallet, owing to the pressure placed on the tag: "I guess I would be potentially worried about it getting pressed inside of my wallet accidentally" (P4). Similarly, P10 mentioned, "If my wallet was full of cards ... putting pressure on the spot that needs to be pressed without me actually doing it, it would be working I guess." We noted, however, that several participants were concerned over accidental activation even for RFID-blocking wallets because of the potential for human error and damage. For instance, when given an RFID-blocking wallet, P17 tried orienting the given tag in different configurations to test if the RFID-blocking wallet successfully blocked transmission if the tag remained partially exposed: "What if you mistakenly like put it [partially exposed]...when you're...super busy or something?" P11 expressed similar concerns: "If [the wallet] is like broken or something...I cannot be 100% sure about [RFID blocking]."

b) Perceptible Antenna (Dis)connection Builds Trust in RFID Tag State: Many participants mentioned that the visual cues provided by On-demand RFID helped them understand its state. They found two aspects of the design particularly helpful in this respect: (i) the obvious disconnection in the physical antenna and (ii) the visible liquid switch. Several participants demonstrated their understanding that the antenna disconnection disables the signal transmission. For example, P3 explained: "You could actually see that...the circuit is

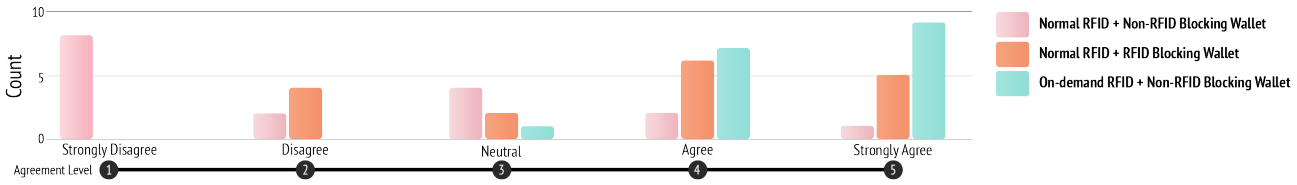

Fig. 5. This chart illustrates the result of the trust-score test conducted in the study's phase 2 regarding the agreement level of the following statement: "The tag is not readable when you don't intend to use the tag. (e.g., when putting it back in your pocket)". As a result, participants expressed higher trust level that On-demand RFID with a non-RFID blocking wallet is not readable when there is no intention to use compared to the other conditions.

being disconnected physically ... That ensures [to] me that [unauthorized RFID reading] is totally blocked."

Additionally, we found that On-demand RFID provided participants with perceptible assurance about the activation state of the tag with visual and physically intuitive cues. Several participants stated that visible liquid movements made it easy to understand when the RFID tag was readable: "The liquid flow is very nice. Because...that's when it's working, and when it's not" (P7). P10 added that the visibility of the liquid movement would allow users to understand how much pressure needs to be applied to activate On-demand RFID, as users can see how far the liquid goes depending on pressure by finger touch.

In contrast, several participants expressed confusion and uncertainty with respect to how RFID-blocking wallets work. Participants had neither a way to easily verify the materials used to make the wallet, nor an intuitive understanding of how the materials could block RFID signals. While participants were generally willing to take a leap of faith and still generally trusted these wallets, this uncertainty reduced their trust in the effectiveness of the RFID-blocking wallet's protection. For example, P2 said, "The material is like a black box so I don't understand how it really works...it's hard for me to fully trust it." Not knowing about the wallet's material status also led P3 to worry about the durability of the wallet, as the material could degrade unknowingly over time.

We also found that the perceptible assurance entailed by On-demand RFID helped participants retain trust even when experiencing a misalignment between tag activation and intention. For example, when some participants observed that the RFID tag remained readable even when inside the RFID-blocking wallet, they felt less confident about the wallet: "If I'm using it with the purpose of keeping it safer and there is a failure mode, then I would feel less confident than using it ...it's going against my expected outcome" (P1). While participants did not directly experience an On-demand RFID tag activating when unintended, participants expressed that it would be easy to debug if such a situation occurred owing to its physically intuitive design. For example, P10 and P12 mentioned that allowing users to see the liquid movement in On-demand RFID could be useful in troubleshooting why On-demand RFID may not work properly (e.g., examining what interrupts liquid movements, checking whether the liquid is dried out.)

c) On-demand RFID Requires More Effort and Attention to Use, But Could Still Be Practical: Some participants expressed reluctance about using On-demand RFID in practice because of the extra steps required to activate the tag. As participants used RFID tags for quick and simple tag readings in their everyday life (e.g., door access), the extra steps to activate the tag could become cumbersome. For example, P11 said, "It's kind of like, unnecessarily...complicated because RFID itself is to make something convenient and quick and fast." In addition, P16 mentioned that it would be challenging to use On-demand RFID without looking at the button location and the liquid movement, which would not be a problem for an RFID-blocking wallet and a normal wallet. Note that this finding was not completely surprising because we specifically aimed to recruit some participants who did *not* have a priori privacy concerns with RFID technologies.

However, other participants expressed enthusiasm for using On-demand RFID in practice. Many of them considered On-demand RFID interactions still easy to learn and use. As P9 said, "You just have to press it not too hard...It's easy enough for anyone to understand." Additionally, the form factor of On-demand RFID appealed to several participants. P17 valued the usage of liquid as a way to create a thin form factor as it eliminated the need for a bulky mechanical switch for connecting the circuit. P15 also envisioned that this technique could be applied to various RFID use cases (e.g., credit card, key fob, etc.) in a manner that would require minimal form factor changes from current RFID tag designs, adding that On-demand RFID would negate the need to buy multiple RFID-blocking wallets or sleeves.

V. Discussion

Our study revealed that people place higher trust in On-demand RFID than commodity RFID tags both with and without an RFID-blocking wallet, largely due to its physically intuitive design, intentional activation, and providing perceptible assurance of state. Moreover, we found that this increase in trust can come with high usability. The core contribution of our work, thus, is the novel application (usable S&P) of known techniques (i.e., using microfluidics to connect/disconnect RFID antennas [12]) to address how to improve end-user trust in RFID sensing systems. In the following subsections, we delve into the factors that influence the trust and usability of On-demand RFID, limitations, and future directions.

A. Increasing Trust with Physically-Intuitive Design

We found that perceptible operations, which users can directly observe and over which they have agency, can help establish trust in using passive RFID technology.

Direct observation of state and state changes was a key driver of trust. In particular, participants found two aspects of the design of On-demand RFID helpful in understanding its operation: (i) the physical antenna disconnection and (ii) the visible fluid movement. The antenna disconnection was compelling evidence to participants that On-demand RFID could not work without intentional activation. Moreover, many participants appreciated that On-demand RFID provided a visual indication of state that was easy to audit and difficult to falsify or misinterpret: the bright conductive ink was either completing the circuit or not. The visible fluid movement further provided users with an intuitive understanding of how much pressure must be applied for the fluid to re-connect the antenna, further bolstering trust.

While visibility drove trust in our participants, we observed opportunities for improvement. There might be situations, for example, where users cannot carefully examine the liquid movement in On-demand RFID, e.g., in low light conditions, or if the user has visual impairments. It would be prudent, therefore, for future explorations to supplement the visual feedback provided by On-demand RFID with secondary forms of feedback such as haptics. For example, Han et al. introduced a novel technique to move a bead inside a microfluidic channel to provide haptic feedback [61]. Building on this technique, we might envision the microfluidic channel in On-demand RFID swelling as it is traversed by the conductive ink. This swelling could provide haptic indications of state that could supplement or eliminate reliance on visual feedback.

Intentional activation also drove trust in our participants. Many of them expressed high confidence that the On-demand RFID would not and could not be activated without active interaction on their part. This firm belief, in turn, convinced participants that it would not be possible for malicious readers to covertly access their On-demand RFID tags. This finding resonates with prior work: Do et al. found that users placed greater trust in an intelligent webcam cover that required manual uncovering and automatic re-covering than in one that automatically covered *and* uncovered [6]. Prior work has also found that intentional powering of microphones can engender user trust in their operation [8], [7]. In short, we add to an emerging stream of work suggesting that sensors must be designed in a manner that is physically intuitive to engender trust.

B. Accidental Activation Reduces Trust

The possibility of accidental activation was the main factor that reduced user trust in using On-demand RFID. Several participants in our study expressed concerns that the antenna of On-demand RFID might be accidentally connected if enough pressure was applied to the button when placed inside a wallet. While they acknowledged that this would likely be a rare occurrence, the mere possibility was enough to reduce trust for some participants. Accordingly, future design explorations might explore mechanisms that provide assurance that it is not possible to accidentally activate On-demand RFID. For example, setting the button fingertip size and slightly inward compared to its surrounding surface could require a user's intentional press with their finger and prevent accidental press with larger surface contact.

C. On-demand RFID is More Suited to Use-cases that Warrant Heightened S&P Concerns

While users generally found On-demand RFID to be highly usable, it does add a usability burden beyond passive RFID. Accordingly, On-demand RFID should not be used as a blanket replacement for all existing use cases of passive RFID. Privacy concerns are context-dependent [62] and user-dependent. Unsurprisingly, thus, several participants mentioned that their willingness to use On-demand RFID over passive RFID would be contingent on the use case. On-demand RFID may not be the best option for access control to a physical building, for example, since such a scenario generally requires quick interactions involving low-sensitivity information; the additional step to press the button for On-demand RFID may be too much of a hurdle for on-the-go users who need to open a door instantaneously. On the contrary, cases where preventing data breaches is a priority, such as financial information stored in contactless payment systems and credit cards, might be more suitable for applying On-demand RFID. It would be prudent to explore, in future work, who would be willing to adopt On-demand RFID for which use cases and which contexts.

1) Use cases for On-demand RFID: The prevalence of passive RFID technology has skyrocketed for a wide range of daily use cases, including payment systems, door access to physical private spaces, and location tracking. For which use-cases might On-demand RFID be most promising? Microfluidic channel designs can be flexibly structured within a relatively thin chip, enabling a wide spectrum of different form factors and sizes [10], [45]. Furthermore, channel design can be customized according to the button size and position of On-demand RFID. This structural flexibility allows for a wide variety of interactions and form factors that can be tuned according to users' needs.

One promising potential use case of On-demand RFID is in contactless payment cards, as contactless payment technology has increasingly become ubiquitous to avoid frequent physical contact with common surfaces between different individuals. Given its thin form factor, On-demand RFID could be integrated into existing payment cards, as suggested by our participants.

Additionally, On-demand RFID could address interference problems caused by stacking multiple cards inside one wallet. When multiple cards with RFID tags are placed in the same wallet, these cards can interfere with one another when tapped against a reader as each of the cards will send back their data via RF signals simultaneously and in similar locations [63]. As a result, users must manually remove the pertinent card from the stack and tap it separately against a reader

for it to operate as expected. However, with On-demand RFID, this interference problem could be resolved: one could imagine integrating multiple On-demand RFID tags inside a single card, with separate buttons for each tag. This way, a user can select which RFID tag should be activated by selectively pressing the respective button. This design could allow for physically reconfigurable RFID tags—something already digitally plausible and deployed in electronic payment systems (e.g., changing credit cards on Apple Pay).

Finally, On-demand RFID could also eliminate the need for a user to carry a card or a wallet altogether. For example, it could be fabricated into a separate physical instrument that fits onto a key ring instead; with such an accessory, users could simply press the button directly from their key chain only when they want to use a specific tag.

D. Limitations and Future Work

In this section, we will discuss the remaining challenges and future directions to make On-demand RFID deployable in practice.

1) On-demand RFID for Different RF Ranges.: We implemented On-demand RFID based on UHF technology as a proof-of-concept, inspired by the approach taken by Sun et al. [10]. In practice, however, many RFID applications use not only the UHF range but also the high-frequency (HF) and low-frequency (LF) range. While we have not covered the implementation of HF and LF range, HF and LF tags could be used to implement On-demand RFID as suitable for our target use cases, such as building access badges. However, we would like to note that these ranges would require further technical exploration to apply the On-demand RFID technique to more daily use cases. Particularly, as the sensitivity of reading LF and HF tags differs from UHF tags, it would be essential to explore tuning different parameters, such as a gap between the severed antenna traces and the conductive liquid amount that bridges the gap [10].

2) Ecological Validity.: In our controlled study, we found that participants expressed higher trust in using On-demand RFID than a commodity RFID tag both with and without using an RFID-blocking wallet. However, there could be factors that affect users' trust in On-demand RFID that manifest "in the wild" that our study did not capture. For example, durability and reliability are also critical determinants of trust: if a system is broken and not reliably functioning, its operations may work against users' expectations and thus reduce trust. The current On-demand RFID prototype is susceptible to accidental triggering. For example, we found that placing a finger on top of the disconnected antenna of the current prototype can also re-connect the antenna and activate the RFID tag. Also, since we manually assembled each On-demand RFID tag, the sensitivity of the tag varied depending on fabrication quality. We also observed that the water that was used as conductive liquid in our prototype evaporated over time, requiring occasional refilling (echoing the findings by Sun el al. [10]). These limitations can reduce the durability and reliability of On-demand RFID for long-term use, which could reduce trust. Accordingly, for field deployments, it is necessary to further engineer and fine-tune the design and performance of On-demand RFID to reduce unintentional tag activation, and to improve durability and reliability over an extended period of time and over a wide range of environmental conditions. Many of these challenges are fixable through engineering and fabrication improvements.

3) Alternative Designs for Physically-intuitive RFIDs.: Finally, we note that there could be alternative designs that meet the physically-intuitive design requirements we discussed in Section III-A. Our goal in this paper was *not* to exhaustively explore this design space, but to demonstrate that, by using those requirements as guide, it is possible to design trustworthy RFID chips. To that end, we implemented and evaluated one such design that leverages microfluidic technology — On-demand RFID. Moreover, we found clear evidence that On-demand RFID builds trust and addresses users' S&P concerns against unauthorized passive RFID tag readings in its use of physically-intuitive design principles. Future work might explore other physically-intuitive designs for RFID chips to improve end-user trust.

VI. Conclusion

We designed and implemented On-demand RFID to increase user trust and agency over passive RFID technologies, which elicit S&P concerns ranging from employee surveillance to theft of financial information [4]. Extending prior work on building trustworthy sensors [6], [7], [8], On-demand RFID employs physically-intuitive design to provide users with agency over RFID chip activation and provide perceptible assurance of sensing state. On-demand RFID tags are deactivated by default and can be reactivated intentionally when the user presses a button that directs conductive liquid through a fabricated microfluidic channel that bridges its severed RFID antenna. Through a controlled, within-subjects evaluation with 17 participants, we found that users trusted On-demand RFID significantly more than not just a passive RFID tag on its own, but also one paired with an RFID-blocking wallet. Our design further contributes to a burgeoning chorus of work showing that it is possible to build usable, trustworthy sensing systems through physically-intuitive design.

Acknowledgment

This work was generously funded, in part, by NSF SaTC Grant #2316294. We thank Lining Yao, Dinesh K. Patel, Humphrey Yang, Daehwa Kim, Jung Wook Park, Alex Adams, Wei Sun, and Cassandra Martin for early design discussion, GVU Prototyping Lab for prototype tool support, and Chris Harrison and Vimal Mollyn for test equipment support.

Disclaimer

This presentation was prepared for informational purposes by the Global Technology Applied Research center of JP-Morgan Chase & Co. This presentation is not a product of the Research Department of JPMorgan Chase & Co. or its

affiliates. Neither JPMorgan Chase & Co. nor any of its affiliates makes any explicit or implied representation or warranty and none of them accept any liability in connection with this presentation, including, without limitation, with respect to the completeness, accuracy, or reliability of the information contained herein and the potential legal, compliance, tax, or accounting effects thereof. This document is not intended as investment research or investment advice, or as a recommendation, offer, or solicitation for the purchase or sale of any security, financial instrument, financial product or service, or to be used in any way for evaluating the merits of participating in any transaction.

REFERENCES

[1] M. Weiser, "The computer for the 21 st century," *Scientific american*, vol. 265, no. 3, pp. 94–105, 1991.

[2] J. King and A. Selcukoglu, "Where's the beep? a case study of user misunderstandings of rfid," in *2011 IEEE International Conference on RFID*. IEEE, 2011, pp. 192–199.

[3] Statista, "Rfid (radio frequency identification) technology market revenue worldwide from 2014 to 2025," 2020, (Accessed on 05/21/2022). [Online]. Available: https://www.statista.com/statistics/781338/global-rfid-technology-market-revenue/

[4] A. C. L. Union, "Rfid position statement," 2003. [Online]. Available: https://www.aclu.org/other/rfid-position-statement

[5] P. Kennedy, "Card format passport; changes to passport fee schedule," December 2007, https://www.federalregister.gov/documents/2007/12/31/E7-25422/card-format-passport-changes-to-passport-fee-schedule (Accessed on 01/13/2024).

[6] Y. Do, J. W. Park, Y. Wu, A. Basu, D. Zhang, G. D. Abowd, and S. Das, "Smart webcam cover: Exploring the design of an intelligent webcam cover to improve usability and trust," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 5, no. 4, pp. 1–21, 2021.

[7] Y. Do, N. Arora, A. Mirzazadeh, I. Moon, E. Xu, Z. Zhang, G. D. Abowd, and S. Das, "Powering for privacy: Improving user trust in smart speaker microphones with intentional powering and perceptible assurance," in *32nd USENIX Security Symposium (USENIX Security 23)*, 2023, pp. 2473–2490.

[8] I. Ahmad, T. Akter, Z. Buher, R. Farzan, A. Kapadia, and A. J. Lee, "Tangible privacy for smart voice assistants: Bystanders' perceptions of physical device controls," *Proceedings of the ACM on Human-Computer Interaction*, vol. 6, no. CSCW2, pp. 1–31, 2022.

[9] K. Koscher, A. Juels, V. Brajkovic, and T. Kohno, "Epc rfid tag security weaknesses and defenses: passport cards, enhanced drivers licenses, and beyond," in *Proceedings of the 16th ACM conference on Computer and communications security*, 2009, pp. 33–42.

[10] W. Sun, Y. Chen, Y. Chen, X. Zhang, S. Zhan, Y. Li, J. Wu, T. Han, H. Mi, J. Wang *et al.*, "Microfluid: A multi-chip rfid tag for interaction sensing based on microfluidic switches," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 6, no. 3, pp. 1–23, 2022.

[11] H. Hutchinson, W. Mackay, B. Westerlund, B. B. Bederson, A. Druin, C. Plaisant, M. Beaudouin-Lafon, S. Conversy, H. Evans, H. Hansen *et al.*, "Technology probes: inspiring design for and with families," in *Proceedings of the SIGCHI conference on Human factors in computing systems*, 2003, pp. 17–24.

[12] R. Kumar, "A note from the uist 2021 pc chairs," May 2021. [Online]. Available: https://medium.com/acm-uist/a-note-from-the-uist-2021-pc-chairs-6a30df14f33b

[13] J. R. Smith, A. P. Sample, P. S. Powledge, S. Roy, and A. Mamishev, "A wirelessly-powered platform for sensing and computation," in *International Conference on Ubiquitous Computing*. Springer, 2006, pp. 495–506.

[14] A. P. Sample, D. J. Yeager, P. S. Powledge, A. V. Mamishev, and J. R. Smith, "Design of an rfid-based battery-free programmable sensing platform," *IEEE transactions on instrumentation and measurement*, vol. 57, no. 11, pp. 2608–2615, 2008.

[15] K. P. Fishkin, B. Jiang, M. Philipose, and S. Roy, "I sense a disturbance in the force: Unobtrusive detection of interactions with rfid-tagged objects," in *International Conference on Ubiquitous Computing*. Springer, 2004, pp. 268–282.

[16] S. Pradhan, E. Chai, K. Sundaresan, L. Qiu, M. A. Khojastepour, and S. Rangarajan, "Rio: A pervasive rfid-based touch gesture interface," in *Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking*, 2017, pp. 261–274.

[17] A. P. Sample, D. J. Yeager, and J. R. Smith, "A capacitive touch interface for passive rfid tags," in *2009 IEEE International Conference on RFID*. IEEE, 2009, pp. 103–109.

[18] H. Li, E. Brockmeyer, E. J. Carter, J. Fromm, S. E. Hudson, S. N. Patel, and A. Sample, "Paperid: A technique for drawing functional battery-free wireless interfaces on paper," in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, 2016, pp. 5885–5896.

[19] H. Jin, J. Wang, Z. Yang, S. Kumar, and J. Hong, "Rf-wear: Towards wearable everyday skeleton tracking using passive rfids," in *Proceedings of the 2018 ACM International Joint Conference and 2018 International Symposium on Pervasive and Ubiquitous Computing and Wearable Computers*, 2018, pp. 369–372.

[20] J. Wang, C. Pan, H. Jin, V. Singh, Y. Jain, J. I. Hong, C. Majidi, and S. Kumar, "Rfid tattoo: A wireless platform for speech recognition," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 3, no. 4, pp. 1–24, 2019.

[21] J. Gummeson, J. Mccann, C. Yang, D. Ranasinghe, S. Hudson, and A. Sample, "Rfid light bulb: Enabling ubiquitous deployment of interactive rfid systems," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 1, no. 2, pp. 1–16, 2017.

[22] M. Langheinrich, "A survey of rfid privacy approaches," *Personal and Ubiquitous Computing*, vol. 13, pp. 413–421, 2009.

[23] F. Vara-Orta, "Students will be tracked via chips in ids," May 2012. [Online]. Available: https://www.mysanantonio.com/news/education/article/Students-will-be-tracked-via-chips-in-IDs-3584339.php

[24] T. Simmons, "3 solutions to electronic car theft, a continuing threat to high-end toronto automobiles — cbc news," https://www.cbc.ca/news/canada/toronto/electronic-car-theft-rising-1.5138877, May 2019, (Accessed on 07/27/2023).

[25] S. Spiekermann and S. Evdokimov, "Critical rfid privacy-enhancing technologies," *IEEE Security & Privacy*, vol. 7, no. 2, pp. 56–62, 2009.

[26] J. Wang, J. Zhang, R. Saha, H. Jin, and S. Kumar, "Pushing the range limits of commercial passive {RFIDs}," in *16th USENIX Symposium on Networked Systems Design and Implementation (NSDI 19)*, 2019, pp. 301–316.

[27] Apple, Oct 2022. [Online]. Available: https://support.apple.com/en-us/HT212733

[28] I. Ahmad, R. Farzan, A. Kapadia, and A. J. Lee, "Tangible privacy: Towards user-centric sensor designs for bystander privacy," *Proceedings of the ACM on Human-Computer Interaction*, vol. 4, no. CSCW2, pp. 1–28, 2020.

[29] D. Machuletz, S. Laube, and R. Böhme, "Webcam covering as planned behavior," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 2018, pp. 1–13.

[30] J. Steil, M. Koelle, W. Heuten, S. Boll, and A. Bulling, "Privaceye: privacy-preserving head-mounted eye tracking using egocentric scene image and eye movement features," in *Proceedings of the 11th ACM symposium on eye tracking research & applications*, 2019, pp. 1–10.

[31] J. Lau, B. Zimmerman, and F. Schaub, "Alexa, are you listening? privacy perceptions, concerns and privacy-seeking behaviors with smart speakers," *Proceedings of the ACM on human-computer interaction*, vol. 2, no. CSCW, pp. 1–31, 2018.

[32] H. Jin, B. Guo, R. Roychoudhury, Y. Yao, S. Kumar, Y. Agarwal, and J. I. Hong, "Exploring the needs of users for supporting privacy-protective behaviors in smart homes," in *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, 2022, pp. 1–19.

[33] NPR and E. Research, "The smart audio report," June 2022, https://www.nationalpublicmedia.com/uploads/2020/04/The-Smart-Audio-Report_Spring-2020.pdf (Accessed on 01/31/2023).

[34] V. Chandrasekaran, S. Banerjee, B. Mutlu, and K. Fawaz, "{PowerCut} and obfuscator: An exploration of the design space for {Privacy-Preserving} interventions for smart speakers," in *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*, 2021, pp. 535–552.

[35] N. Marquardt, A. S. Taylor, N. Villar, and S. Greenberg, "Rethinking rfid: awareness and control for interaction with rfid systems," in *Pro-*

ceedings of the SIGCHI Conference on Human Factors in Computing Systems, 2010, pp. 2307–2316.
[36] G. Karjoth and P. A. Moskowitz, "Disabling rfid tags with visible confirmation: clipped tags are silenced," in *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, 2005, pp. 27–30.
[37] A. Czeskis, K. Koscher, J. R. Smith, and T. Kohno, "Rfids and secret handshakes: Defending against ghost-and-leech attacks and unauthorized reads with context-aware communications," in *Proceedings of the 15th ACM conference on Computer and communications security*, 2008, pp. 479–490.
[38] Z. Jiang and F. Yang, "Reconfigurable sensing antennas integrated with thermal switches for wireless temperature monitoring," *IEEE Antennas and Wireless Propagation Letters*, vol. 12, pp. 914–917, 2013.
[39] N. Saxena, M. B. Uddin, J. Voris, and N. Asokan, "Vibrate-to-unlock: Mobile phone assisted user authentication to multiple personal rfid tags," in *2011 IEEE International Conference on Pervasive Computing and Communications (PerCom)*. IEEE, 2011, pp. 181–188.
[40] K. Katsuragawa, J. Wang, Z. Shan, N. Ouyang, O. Abari, and D. Vogel, "Tip-tap: battery-free discrete 2d fingertip input," in *Proceedings of the 32nd Annual ACM Symposium on User Interface Software and Technology*, 2019, pp. 1045–1057.
[41] R.-H. Liang, M.-J. Hsieh, J.-Y. Ke, J.-L. Guo, and B.-Y. Chen, "Rfi-match: Distributed batteryless near-field identification using rfid-tagged magnet-biased reed switches," in *Proceedings of the 31st Annual ACM Symposium on User Interface Software and Technology*, 2018, pp. 473–483.
[42] M.-J. Hsieh, R.-H. Liang, D.-Y. Huang, J.-Y. Ke, and B.-Y. Chen, "Rfibricks: Interactive building blocks based on rfid," in *Proceedings of the 2018 CHI conference on human factors in computing systems*, 2018, pp. 1–10.
[43] H. Ishii, "Tangible bits: beyond pixels," in *Proceedings of the 2nd international conference on Tangible and embedded interaction*, 2008, pp. xv–xxv.
[44] P. Dourish, R. E. Grinter, J. Delgado De La Flor, and M. Joseph, "Security in the wild: user strategies for managing security as an everyday, practical problem," *Personal and Ubiquitous Computing*, vol. 8, pp. 391–401, 2004.
[45] H. Mor, T. Yu, K. Nakagaki, B. H. Miller, Y. Jia, and H. Ishii, "Venous materials: towards interactive fluidic mechanisms," in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 2020, pp. 1–14.
[46] W. Sun, Y. Chen, S. Zhan, T. Han, F. Tian, H. Wang, and X.-D. Yang, "Relectrode: A reconfigurable electrode for multi-purpose sensing based on microfluidics," in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 2021, pp. 1–12.
[47] Y. Tokuda, D. R. Sahoo, M. Jones, S. Subramanian, and A. Withana, "Flowcuits: Crafting tangible and interactive electrical components with liquid metal circuits," in *Proceedings of the Fifteenth International Conference on Tangible, Embedded, and Embodied Interaction*, 2021, pp. 1–11.
[48] D. J. Wilson, F. J. Martín-Martínez, and L. F. Deravi, "Wearable light sensors based on unique features of a natural biochrome," *ACS sensors*, vol. 7, no. 2, pp. 523–533, 2022.
[49] V. D. of Motor Vehicles, "How to use your vermont edl," Aug 2014, https://youtu.be/tBrVAfdE0GA (Accessed on 07/17/2024).
[50] J. R. Lewis and J. Sauro, "Item benchmarks for the system usability scale." *Journal of Usability Studies*, vol. 13, no. 3, 2018.
[51] D. H. McKnight and N. L. Chervany, "What is trust? a conceptual analysis and an interdisciplinary model," 2000.
[52] K. O'Hara, "A general definition of trust," 2012.
[53] K. Blomqvist, "The many faces of trust," *Scandinavian journal of management*, vol. 13, no. 3, pp. 271–286, 1997.
[54] M. Friedman, "The use of ranks to avoid the assumption of normality implicit in the analysis of variance," *Journal of the american statistical association*, vol. 32, no. 200, pp. 675–701, 1937.
[55] F. Wilcoxon, "Individual comparisons by ranking methods. biom. bull., 1, 80–83," 1945.
[56] A. Field, "Discovering statistics using spss (third edit)," *London and New York: Sage*, 2009.
[57] V. Braun and V. Clarke, *Thematic analysis.* American Psychological Association, 2012.
[58] K. M. MacQueen, E. McLellan, K. Kay, and B. Milstein, "Codebook development for team-based qualitative analysis," *Cam Journal*, vol. 10, no. 2, pp. 31–36, 1998.
[59] J. Corbin and A. Strauss, *Basics of qualitative research: Techniques and procedures for developing grounded theory*. Sage publications, 2014.
[60] N. McDonald, S. Schoenebeck, and A. Forte, "Reliability and inter-rater reliability in qualitative research: Norms and guidelines for cscw and hci practice," *Proceedings of the ACM on human-computer interaction*, vol. 3, no. CSCW, pp. 1–23, 2019.
[61] T. Han, S. Bansal, X. Shi, Y. Chen, B. Quan, F. Tian, H. Wang, and S. Subramanian, "Hapbead: on-skin microfluidic haptic interface using tunable bead," in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 2020, pp. 1–10.
[62] P. E. Naeini, S. Bhagavatula, H. Habib, M. Degeling, L. Bauer, L. F. Cranor, and N. Sadeh, "Privacy expectations and preferences in an {IoT} world," in *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, 2017, pp. 399–412.
[63] D.-Y. Kim, H.-G. Yoon, B.-J. Jang, and J.-G. Yook, "Interference analysis of uhf rfid systems," *Progress In Electromagnetics Research B*, vol. 4, pp. 115–126, 2008.