Tracking, But Make It Offline: The Privacy Implications of Scanning QR Codes Found in the World

Rayaan Siddiqi*, Shubham Singh*, Lenore Zuck, Chris Kanich
University of Illinois Chicago
{*rsiddi29, ssing57, zuck, ckanich*}*@uic.edu*
[*]*Equal Contribution*

***Abstract*—QR Codes have become a pervasive mechanism for encoding machine-readable digital data in the offline world. As the Internet age has taught us, mechanisms that become pervasive very often engender privacy concerns regarding their use. As such, here we conduct an investigation of the privacy implications of the QR Code ecosystem as it exists today.**

We find that there are several shortener services with substantial popularity, and investigate the extent to which these shortener services conduct various types of tracking of individuals who interact with the created QR Codes. Additionally, we collect 948 QR codes posted within the world, and evaluate them for various types of tracking as well. Overall, we find no evidence that QR codes are a substantial or unique privacy threat when compared to other link sharing mechanisms available online. Even so, the theoretical potential for surreptitious tracking exists, and more in depth study of the QR Code ecosystem will allow for deeper investigation of the relationship between online and offline tracking.

***Index Terms*—QR codes, URL shorteners, tracking, privacy**

1. Introduction

The widespread adoption of certain technologies often leads to privacy concerns, as demonstrated by the emergence of the digital era. More concerningly, the ease with which economies of scale can be created online has led to substantial concentrations of data by large Internet companies. At the same time, QR codes are exploding in popularity as a means of bridging the offline and online worlds [1], [2]. Particularly, studying QR codes is important now due to their widespread adoption and usage during the COVID-19 pandemic. As they become a more integral part of our daily lives, it's crucial to understand the potential risks and vulnerabilities associated with their usage, especially when it comes to the potential security concerns surrounding the data they collect and transmit.

Thus, this research investigates the extent to which the privacy implications of the use of QR codes in the offline world has become privacy invasive and concentrated.

QR codes are similar to shortened links as they don't indicate the content of the link. *Dynamic QR codes* are created by combining shortened link services and QR codes, allowing for longer URLs and the ability to change the destination of a QR code after it has been posted. They also provide additional analytics for the link poster.

Most people use third-party QR code generators instead of on-device ones, as they are more widely available and easier to use. These services convert URLs into scannable QR codes, with many offering dynamic QR codes instead of just encoding the given URL. This allows two main benefits for the QR code creator: they can change the destination URL at any time, and the QR code hosting service can provide user analytics for the QR code scans. Besides analytics, dynamic QR code providers can track users and collect personal information such as the location of where a QR code is scanned (city, country), the browser type, and the device performing the scan.

These properties, when combined with QR codes' newfound popularity, elicit several questions relative to consumer privacy and protection. In this paper, we conduct an investigation focused on the offline aspect of QR code usage, with three main contributions: first, we collect 948 QR codes in the offline world using a custom collection mechanism; second, we investigate each of those URLs for their privacy implications as if a user had scanned them; finally, we investigate 37 popular QR code shortener services to determine the extent to which they respect consumer privacy. Overall, we found that the QR code ecosystem does not significantly detract from users' online or geographic privacy compared to the online status quo; further discussion and conclusions can be found in § 6.

2. Related Work

While there is minimal prior work on QR codes in the offline world, there is abundant prior work on the privacy and security concerns related to URL shortening and QR codes in the online context.

URL Shortening. URL shortening services obfuscate the primary destination URL by providing a short, concise URL and more accessible to type in a browser compared to the conventional URL. They also allow short URL creators to gather analytics on the users who click on the short

This material is based upon work supported by the National Science Foundation under Grant Nos. CNS-1801644, CCS-2140207, and SHF-1918429, by the Department of Defense under Grant No. W911NF2010310, and the Discovery Partners Institute.

URLs. However, for those reasons, attackers could use such services for malicious purposes. Maggi et al. [3] analyze the popular URL shortening services and found that most of them do not employ active measures to flag malicious destination URL. They developed a browser add-on to collect a large-scale short URL dataset and found that only a small fraction of the add-on users come across malicious short URLs [3]. Similar studies analyze the time taken by Bitly, a popular URL shortening service, to remove malicious short URLs [4] and their prevalence on Twitter [5]. Other works focus on ad-based URL shortening services, where a user is shown advertisements before she can access the destination URL when she clicks on a short URL [6], [7]. The intermediate pages show lure buttons to confuse the user into clicking on an advertisement and such services generate a lot of requests to malicious domains [7]. Although our work focuses on the QR codes collected from the real world, many of the decoded URLs in our dataset are short URLs. We want to study the advantages an attacker might have when using a short URL behind a QR code.

QR Codes. Prior studies identify scenarios in which QR codes can be misused by malicious actors [8], [9]. Nowadays, QR codes are primarily used to render websites accessible on mobile devices. Prior work has looked into the security measures QR code scanning apps employ to prevent users from harm and found that they are mostly ineffective [10], [11]. Furthermore, Dabrowski et al. [12] introduce an attack by generating a QR code within a QR code and find inconsistent behavior among scanning apps on iOS and Android. In absence of a standard decoding algorithm, the non-uniformity of QR decoding implementation could be used for discriminatory, targeted advertisements [12].

Researchers have also conducted user studies to understand why people scan QR codes in the wild and found that curiosity is one of the primary reasons [13], [14]. There exist two works in QR code literature that are highly relevant to us. The first looks at the scan logs of a popular scanning application on multiple mobile platforms [15]. The second collects the QR codes hosted on the websites using a web crawler [16]. Both studies collect a large-scale dataset of QR codes and find a relatively low number of QR codes in the wild are being used for malicious intents [15], [16]. Our work collects the QR codes in the wild using mobile devices, and our analysis supports their findings in the post-pandemic world.

3. Data Collection

We designed a data collection mechanism that minimizes latency when using a mobile phone to scan QR codes found in the offline world, and maximize the amount of relevant data collected about both the online and offline components of each QR Code.

Offline Data Collection. Outside of a few QR codes collected during testing, our dataset was exclusively collected using an iOS Shortcut. iOS Shortcuts allow Scratch-style drag-and-drop automation of various operations. This shortcut activates the camera to search for QR codes in its field of view, collects the current geolocation (both coordinates and an Apple-provided reverse geocoded street address), and sends the decoded QR Code alongside the geolocation to a Google Cloud Run endpoint for online data collection. Once the relevant permissions have been granted and the shortcut is saved to a lock screen widget, the entire process of collecting and uploading a geolocated QR code can take as few as 3 seconds. The authors and their colleagues collected the data, with the majority (75%) of scans being obtained during the peak of the COVID-19 pandemic. Though there is a large concentration of scans collected in the Chicago area, QR codes were collected in other regions as well as shown in map Fig. 2.

Online Data Collection. Every time the Google Cloud Run endpoint receives a valid submission, it records a visit to the given URL using Puppeteer, including records of every HTTP request made, the initiator for each request, and a screenshot of the resulting page. These results are persisted to a combination Postgres database / object store using the Supabase platform.

4. QR Code Shortener Services

While QR Codes can be shortened using any number of mechanisms, there is a thriving ecosystem of QR Code shortening services available on the web. We focus on 37 QR code shortener services which is the union of the top 25 shortener services found from a Google search of “QR code generator” in August, 2022 along with shortener services from our dataset which were not originally examined. In this section we explore the different options these services provide for users to create QR codes and the privacy implications associated with them.

4.1. Dynamic vs. Static QR Codes

When a dynamic QR code is scanned and opened in a browser, the first request from the device goes to the domain of the QR code service provider. The service provider then commonly redirects the user to the destination page by sending an HTTP 302 status response.

Table 1 shows a list of 37 free QR code generators we analyze. For each, we visit the website and attempt to create both a static and dynamic QR code if possible. Once we generate the QR code, we scan the QR code and inspect the decoded URL. If the decoded URL matches the input URL, we confirm that it is a static QR code. Likewise, if the created QR code is a shortened URL, we treat the QR code as dynamic. We also examine if we, as QR code creators, can opt in or opt out of the creation of a dynamic QR code (column 3). Finally, we specify how popular the QR code generator website is by listing the rank of the service when we searched for “QR code generator” on Google. To avoid personalization of the results, we used a private browser window for the Google search. Moreover, we examined the top 100 search results, and if the shortener service was not ranked within the top 100 hits for our search, then it was marked ‘unranked’.

Shortener Website	**Dynamic Hostname**	**Signup required?**	**Dynamic available?**	**Dynamic Subscription?**	**Search Engine Ranking**
www.qr-code-generator.com	qrco.de	✓	✓	◐	1
goqr.me	x-qr.net	✗	✓	◐	2
www.qrcode-monkey.com/#		✗	✓	◐	3
www.adobe.com/express/feature/image/qr-code-generator		✓	✗	○	4
www.qrstuff.com	qrs.ly	✗	✓	◑	6
qrd.by	qrd.by	✓	✓	◐	7
qrcode.tec-it.com/en		✗	✗	○	8
www.beaconstac.com	qrcodes.pro	✓	✓	◐	9
www.canva.com/apps/qr-code		✓	✗	○	13
me-qr.com	me-qr.com	✗	✓	●	15
www.unitag.io	eqrco.de	✗	✓	●	17
www.qrcode-tiger.com	qr1.be	✓	✓	◐	20
qrexplore.com		✗	✗	○	26
www.barcodesinc.com/generator/qr/		✗	✗	○	30
qrcode.kaywa.com		✓	✓	◑	34
www.the-qrcode-generator.com	qr.page	✓	✓	◐	40
flowcode.com	flowcode.com	✓	✓	●	49
scanova.io	scnv.in	✗	✓	◑	53
www.wix.com/tools/qr-code-generator		✗	✗	○	58
uqr.me	uqr.to	✓	✓	●	63
qr-creator.com/shorten.php	bit.ly	✗	✓	◐	73
qrfy.mobi/my-qr-codes	qrfy.com	✓	✓	●	74
qr.io	qr.link	✓	✓	◐	77
qrcode.studio					81
brandshareus.qrd.by		✗	✗	○	Unranked
create.wa.link	wa.link	✗	✓	●	Unranked
delivr.com/qr-code-generator	delivr.com	✓	✓	●	Unranked
linkmngr.com	linkmn.gr	✓	✓	●	Unranked
linktr.ee	linktr.ee	✓	✓	●	Unranked
qr1.be		✓	✓	◐	Unranked
qrco.de	qrco.de	✓	✓	◐	Unranked
short.io	<unique-id>.short.gy	✓	✓	●	Unranked
www.onelink.to	www.onelink.to	✓	✓	●	Unranked
www.qrcodechimp.com	qrcc.me	✓	✓	◐	Unranked
sqrcode.com/site/signup					Unranked
qr30.cn					Unranked
www.logaster.com/qr-code-generator					Unranked

TABLE 1: Details for the QR code generator websites. ● indicates websites that *only* allow the creation of dynamic QR codes, ○ indicates websites that have no such option. ◐ websites allow creators to *opt-in* for a dynamic QR code, whereas ◑ is *opt-out*.

4.2. Shortener Investigation

While Table 1 lists a large variety of shortener services, there is substantial concentration in the QR shortener marketplace. Bitly, the well-known URL shortener service, owns multiple QR code services with high search engine ranking. Interestingly, they have made QR codes a core highlight of their current and future growth strategy [17].

When investigating the analytics information provided by dynamic QR code services, we found that the vast majority of them report city level geolocation, OS, Browser, and total scans. From a privacy perspective, this is certainly invasive; however, if a user has chosen to visit a given website, each of those pieces of information is available to those websites as well. Thus, the main concern is not the absolute risk to privacy for any given user scanning QR codes, but rather the aggregation of data by the dynamic QR code providers. Bitly provides a perfect example here: because they own the plurality of all scanned dynamic QR codes in our dataset, rather than that data being distributed among the dozens of entities who posted those QR codes, all of that data is centralized with Bitly. This centralization is one of the main concerns we see in the current offline world QR code usage ecosystem.

Within our exploration of this data, there were a handful of noteworthy discoveries. *me-qr.com* and *unitag.io* do not require login and returns a QR code when given a URL, but does not inform the user that the QR code does not encode the given URL but rather a URL under their control. Similarly, *qrstuff.com* provides a dynamic URL by default without informing the user, and only allows opting out of the dynamic URL after several pages of QR code configuration. Notably, *beaconstac.com* provides the option to collect a browser-provided geolocation before redirection, as well as monetization through a short interstitial page of advertisements. While JavaScript based redirections are more concerning from a privacy perspective (because they allow the QR code creation service to include additional tracking libraries on the intermediate page), this was the only instance we observed in our dataset.

5. QR Codes Statistics

Statistic	Count
Total Scans	948
Valid Scans	857
Unique Valid Scans	728
Unique Domains	401
Unique Street Addresses	556

TABLE 2: Dataset details

Table 2 provides an overview of the data we collected, where valid encodes a URL we can visit. The remainder of this section investigates the results of visiting these URLs. Our dataset contains the QR codes scanned for about 17 months, between July 29, 2021 to December 31st, 2022.

5.1. Geographic Locations of QR Scans

URL	Count
https://play.google.com/store/apps/details?id=com.ca.fantuan.customer	3
https://www.slickmenus.com/	2
https://www.slickmenus.com/restaurants/strings-ramen-chinatown-chicago-il/menu?utm_medium=order&utm_source=website	2
https://viennabeefprod.b2clogin.com/viennabeefprod.onmicrosoft.com/B2C_1A_SIGNUP_SIGNIN<truncated>	2
https://dreamsforkids.org/holiday-for-hope/	2
https://insomniacookies.com/cookiemagic	2
https://foxtrotco.com/?utm_source=instore&utm_medium=storesign&utm_campaign=downloadapp	2

TABLE 3: Most common destination URLs.

One noteworthy implication of posting unique QR codes in the offline world in static locations is that they can be used to circumvent location sharing prevention by the scanner: for instance, even if a user refuses to allow geolocation via JavaScript and hides their local IP address via TOR or a VPN, a QR code poster can record the location the QR code was posted, and be confident that the scanner was in that place at that time.

We can conduct two analyses to investigate this hypothesis: first, we can determine the extent to which unique QR codes posted in different locations redirect to the same destination URL. The instances we found are in Table 3. As an example, the Fantuan App was advertised via three unique QR codes, each with a different random string in the decoded URL, redirecting the user to the Google Play Store page of the Fantuan Delivery app. As Fantuan is a food delivery app, they are likely recording which of their client restaurants elicit scans (potentially for a reimbursement/bonus program), which could be considered a form of QR-based location tracking as described above. The other examples also include retail chains (Foxtrot and Insomnia Cookies), which likely are intended to conduct similar tracking. Note that this analysis likely severely under-counts the number of websites for which unique QR codes are being generated, because this table only includes web pages for which the final landing URL was identical. It is likely that several other QR codes point to URLs that are canonically the same page, but we leave solving this canonical URL problem as future work.

Second, we can determine the extent to which identical QR codes are scanned at different locations within the offline world. Our dataset has far more examples of this type of QR code: in total, we find 230 identical QR codes. 84 (37%) of those are scanned at a distance greater than 300 feet. Thus, at least in this dataset, it is far more common for QR code users to be uninterested in collecting location information through the QR code scan itself; IP address-based geolocation and active techniques on device could still be employed.

5.2. Redirect Responses

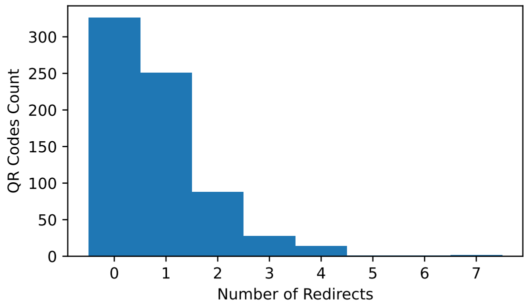

Figure 1: Histogram showing the number of redirect responses a QR code sends before getting to the destination URL.

Redirecting a user's browser is a necessary component of dynamic QR code operation, as well as a technique used for subverting a user's privacy protections [18]. We record the total number of HTTP 3xx redirection responses we receive before an HTTP 200 OK response when we visit the QR code URLs. Among 592 QR codes that respond with redirection, we observe two QR codes receive seven redirection responses before reaching the final destination. We show the count of QR codes and the number of redirection responses in Fig. 1. 251 (42%) QR codes respond with only one redirection status response. This frequency of redirections appears to be in line or even below the amount of redirections seen in shortened URLs collected from the Internet, indicating that there's likely no more redirect based tracking happening in this ecosystem compared to online shortened URLs [19]. Moreover, we went through the redirections of each QR code from our dataset and saw no third-party domains involved, reinforcing the fact that the redirections happened withing a single domain.

5.3. Intent Based Tracking

We dive deeper into the unique QR codes and the tracking behavior that can occur during the journey that starts when a user scans a QR code and ends when she sees the destination page on her device. More specifically, we examine the type of QR code, URL parameters, and first-party and third-party resources loaded on the destination website.

We label QR code tracking in four major categories:

Dynamic QR Code Tracking. If the decoded URL from the QR code is a short URL with the hostname of one of the identified QR code-generating websites.

URL-Based Tracking. If the decoded URL contains parameters to identify where the user comes from, for example `utm_medium, utm_source` or manually created tokens, e.g. `source=qrcode`.

On-Page Tracking. If the destination page loads resources that record user analytics, for example, Google Analytics and Facebook pixel.

Circumstantial Tracking. If the destination page loads third-party resources from servers hosted by companies that conduct large scale online tracking.

We label the QR codes using the above-mentioned rules and show the details in Table 4; more information about the matching rules we used for each category is available in the appendix in Table 5. Note one QR code could employ more than one type of tracking. The most common tracking observed in our dataset was *Circumstantial* tracking, which is attributed to third-party analytic tracking, styling, and/or content resources. In this case, the website creator might not intend to track their users by including these resources, but including these resources allows these large companies to track users. The second highest occurring tracking mechanism is *On-Page* tracking, employed by 61% of the unique valid scans. While unrelated to the QR codes themselves, this is a good baseline for understanding the amount of tracking that QR code users intend to conduct. We notice only a small fraction of QR codes use URL query parameters to track users (*URL-Based*). Finally, about 32% of the scans use dynamic QR codes allowing the creators to gather high-level analytics about users scanning them.

Tracking Type	Count
Dynamic QR Code	235 (32%)
URL-Based	99 (14%)
On-Page	442 (61%)
Circumstantial	500 (69%)

TABLE 4: Unique QR scans and their destination websites that employ user tracking mechanisms.

We calculate the number of tracking mechanisms used by all the unique valid scans, as well as the conditional probabilities of opting in for a dynamic QR code, given a website already employs other tracking mechanisms. We do not consider *Circumstantial* tracking for this. We observe 151 (21%) websites use no tracking mechanisms. 394 (54%) use at least one of them, 167 (23%) use two, 16 (19%) use three, and only 16 (2%) use three of them. We hypothesize since the QR code generation would be the last step after building a website, we can determine the use of QR codes as a tracking vector. The probability of using *Dynamic QR code* tracking given the website uses *URL-Based* tracking is 22%. Similarly, conditioned on the website using *On-Page* tracking, the probability of using *Dynamic QR code* is 29%. These conditional probabilities do not indicate a clear trend toward any preference for using Dynamic QR codes to maximize user tracking.

6. Discussion and Conclusion

While limited in scope compared to online-first analyses of QR codes and link shorteners [3], [4], [6], [8], [9], [19], this study highlights an orthogonal phenomenon: the extent to which the extensive amount of tracking conducted online make its way into the real world. While there are some highlights like the concentration of the link shortening marketplace under Bitly and various link shorteners' dubious practice of providing shortened URLs without informing the user, by and large the QR codes that we collected operate like many links shared between users online.

One natural question arises in this context: why isn't extensive tracking as common in the QR code space compared to the Internet? Our study has limitations, as our collection of offline data is not as comprehensive or longitudinal as online investigations. Our study cannot make claims of statistically random samples, as it is a severely biased convenience sample. Despite these caveats, users seem to prioritize ease of access to a website over considering how they arrived there.

This straightforward usage of QR codes mirrors the lack of significant effort expended to use QR codes in a manner similar to digital advertising: while there are several services offering analytics as part of their QR code generator offerings, we found only one item in our dataset that uses QR codes as an advertising mechanism, and while we did not conduct a comprehensive search, we only saw one service advertised online, `me-qr-city` (dot com) which allows individuals to solicit QR code scans in the real world in exchange for monetization.

We have two hypotheses for why this is so: first, many QR codes are themselves commercial in nature, advertising a product or service. Even though ads for ad-supported services are common online, we did not see this phenomenon in the offline world. Second, and this speaks to our overall findings, the use of QR codes in the offline world simply does not scale similarly to online ventures like link shorteners. This fact likely influences the amount of concentration and sophistication in QR code tracking - the path to and amount of monetization is not substantial enough to warrant significant venture capital investment.

6.1. Future Work

While this project collected a substantial amount of data about the usage of QR codes and particularly their usage for tracking purposes, we did not engage directly with the users of QR codes. Future work which conducts user studies to better understand the tracking and overall intentions of QR code users would help better elucidate the relationship between QR code users, QR code scanners, and dynamic QR code service operators. Additionally, as Bitly continues to focus the growth of its business on creative uses of QR codes, it will be useful to continue investigating any novel, particularly consumer privacy-hostile, uses of QR codes.

References

[1] Insider Intelligence. (2022) US QR code usage statistics (2019-2025). [Online]. Available: https://www.insiderintelligence.com/charts/us-qr-code-user-statistics/

[2] QrTiger. (2022) QR code usage statistics 2022: 443% scan increase and 438% generation boost. [Online]. Available: https://www.qrcode-tiger.com/qr-code-statistics-2022-q1

[3] F. Maggi, A. Frossi, S. Zanero, G. Stringhini, B. Stone-Gross, C. Kruegel, and G. Vigna, "Two years of short URLs internet measurement: Security threats and countermeasures," in *Proceedings of the 22nd International Conference on World Wide Web - WWW '13*. Rio de Janeiro, Brazil: ACM Press, 2013, pp. 861–872.

[4] S. Le Page, G.-V. Jourdan, G. V. Bochmann, J. Flood, and I.-V. Onut, "Using URL shorteners to compare phishing and malware attacks," in *2018 APWG Symposium on Electronic Crime Research (eCrime)*. San Diego, CA: IEEE, May 2018, pp. 1–13.

[5] N. Gupta, A. Aggarwal, and P. Kumaraguru, "Bit.ly/malicious: Deep dive into short URL based e-crime detection," in *2014 APWG Symposium on Electronic Crime Research (eCrime)*. Birmingham, AL, USA: IEEE, Sep. 2014, pp. 14–24.

[6] N. Nikiforakis, F. Maggi, G. Stringhini, M. Z. Rafique, W. Joosen, C. Kruegel, F. Piessens, G. Vigna, and S. Zanero, "Stranger danger: Exploring the ecosystem of ad-based URL shortening services," in *Proceedings of the 23rd International Conference on World Wide Web - WWW '14*. Seoul, Korea: ACM Press, 2014, pp. 51–62.

[7] N. Fukushi, T. Koide, D. Chiba, H. Nakano, and M. Akiyama, "Analyzing Security Risks of Ad-Based URL Shortening Services Caused by Users' Behaviors," in *Security and Privacy in Communication Networks*, J. Garcia-Alfaro, S. Li, R. Poovendran, H. Debar, and M. Yung, Eds. Cham: Springer International Publishing, 2021, vol. 399, pp. 3–22.

[8] K. Krombholz, P. Frühwirt, P. Kieseberg, I. Kapsalis, M. Huber, and E. Weippl, "QR Code Security: A Survey of Attacks and Challenges for Usable Security," in *Human Aspects of Information Security, Privacy, and Trust*, D. Hutchison, T. Kanade, J. Kittler, J. M. Kleinberg, A. Kobsa, F. Mattern, J. C. Mitchell, M. Naor, O. Nierstrasz, C. Pandu Rangan, B. Steffen, D. Terzopoulos, D. Tygar, G. Weikum, T. Tryfonas, and I. Askoxylakis, Eds. Cham: Springer International Publishing, 2014, vol. 8533, pp. 79–90.

[9] R. Focardi, F. L. Luccio, and H. A. M. Wahsheh, "Security Threats and Solutions for Two-Dimensional Barcodes: A Comparative Study," in *Computer and Network Security Essentials*, K. Daimi, Ed. Cham: Springer International Publishing, 2018, pp. 207–219.

[10] H. Yao and D. Shin, "Towards preventing QR code based attacks on android phone using security warnings," in *Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security*, ser. ASIA CCS '13. New York, NY, USA: Association for Computing Machinery, May 2013, pp. 341–346.

[11] R. Dudheria, "Evaluating Features and Effectiveness of Secure QR Code Scanners," in *2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*. Nanjing: IEEE, Oct. 2017, pp. 40–49.

[12] A. Dabrowski, K. Krombholz, J. Ullrich, and E. R. Weippl, "QR Inception: Barcode-in-Barcode Attacks," in *Proceedings of the 4th ACM Workshop on Security and Privacy in Smartphones & Mobile Devices*. Scottsdale Arizona USA: ACM, Nov. 2014, pp. 3–10.

[13] T. Vidas, E. Owusu, S. Wang, C. Zeng, L. F. Cranor, and N. Christin, "QRishing: The Susceptibility of Smartphone Users to QR Code Phishing Attacks," in *Financial Cryptography and Data Security*, D. Hutchison, T. Kanade, J. Kittler, J. M. Kleinberg, F. Mattern, J. C. Mitchell, M. Naor, O. Nierstrasz, C. Pandu Rangan, B. Steffen, M. Sudan, D. Terzopoulos, D. Tygar, M. Y. Vardi, G. Weikum, A. A. Adams, M. Brenner, and M. Smith, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, vol. 7862, pp. 52–69.

[14] N. Kumar, S. Jain, M. Shukla, and S. Lodha, "Investigating Users' Perception, Security Awareness and Cyber-Hygiene Behaviour Concerning QR Code as an Attack Vector," in *HCI International 2022 Posters*, C. Stephanidis, M. Antona, and S. Ntoa, Eds. Cham: Springer International Publishing, 2022, vol. 1583, pp. 506–513.

[15] A. Lerner, A. Saxena, K. Ouimet, B. Turley, A. Vance, T. Kohno, and F. Roesner, "Analyzing the Use of Quick Response Codes in the Wild," in *Proceedings of the 13th Annual International Conference on Mobile Systems, Applications, and Services*. Florence Italy: ACM, May 2015, pp. 359–374.

[16] A. Kharraz, E. Kirda, W. Robertson, D. Balzarotti, and A. Francillon, "Optical Delusions: A Study of Malicious QR Codes in the Wild," in *2014 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*. Atlanta, GA, USA: IEEE, Jun. 2014, pp. 192–203.

[17] Bitly. (2022, Jul.) Bitly QR Code Index H1 2022. Accessed Jan 18th, 2023. [Online]. Available: https://bitly.com/blog/wp-content/uploads/2022/07/Bitly-QR-Code-Index-H1-2022-Report.pdf

[18] The Brave Privacy Team. (2022) "Unlinkable bouncing" for more protection against bounce tracking. [Online]. Available: https://brave.com/privacy-updates/16-unlinkable-bouncing/

[19] M. Koop, E. Tews, and S. Katzenbeisser, "In-depth evaluation of redirect tracking and link usage," *Proceedings on Privacy Enhancing Technologies*, vol. 2020, no. 4, pp. 394–413, 2020.

Dynamic QR Code Tracking	URL Based Tracking	On-Page Tracking	Circumstantial Tracking
flowto.it	=qr	google-analytics	maps.googleapis
qrco.de	/qr/	www.googletagmanager.com	fonts.gstatic
qrs.ly	qr=	googleadservices	fonts.googleapis
qr.page	=qr/track	google.com/adsense	translate.google
qr-code-generator.com/	##-QR	adservice.google.com	google.com/recaptcha
https://www.qrcode-monkey.com/#	qrcode=true	https://www.facebook.com/tr/	www.facebook.com/csp/reporting
https://goqr.me/	/qr_code	connect.facebook.net	fbcdn
https://www.the-qrcode-generator.com/	/applytracking	geolocation.onetrust.com	api.whatsapp
https://www.flowcode.com/	/TRACKING-ID=	cdn.shopify.com/shopifycloud/consent-tracking-api	instagram.com
https://qrcode.kaywa.com		heapanalytic	typekit
https://www.qrcode-tiger.com/		tr.snapchat.com	static.xx.fbcdn.net
https://www.unitag.io/qrcode		analytics.foresee.com/	ups.analytics.yahoo.com
https://www.barcodesinc.com/generator/qr/		pixel.rubiconproject	js.stripe.com
https://qrd.by		pixel.tapad.com	s7.addthis
https://www.qrcodechimp.com/		track.hubspot/	amazonwebservices
https://delivr.com/qr-code-generator		siteimproveanalytics	ajax.googleapis
https://scanova.io		app.quantummetric.com	web-analytics.smile.io
https://qr.io/		static.ads-twitter.com	js.stripe.com
https://qrfy.mobi/my-qr-codes		pixel.sitescout	googleform
https://www.logaster.com/qr-code-generator/		https://phenomtrackapi.phenompeople.com/track	microsoftform
https://scnv.io			analytics.tiktok.com
iwallet			platform.twitter.com/widgets.js
linkmngr			
qrstud.io			
eqrcode			
sqrcode			
uQR.me			
qrcreator			
short.io			
qr.studio			
me-qr.com			

TABLE 5: We specify the criteria to label QR code tracking behavior in 5.3. Authors discussed commonly known resources used to track users based on the resources found in the dataset. For all categories, we do a string matching in the request logs collected via Puppeteer. The searched strings are shown above.

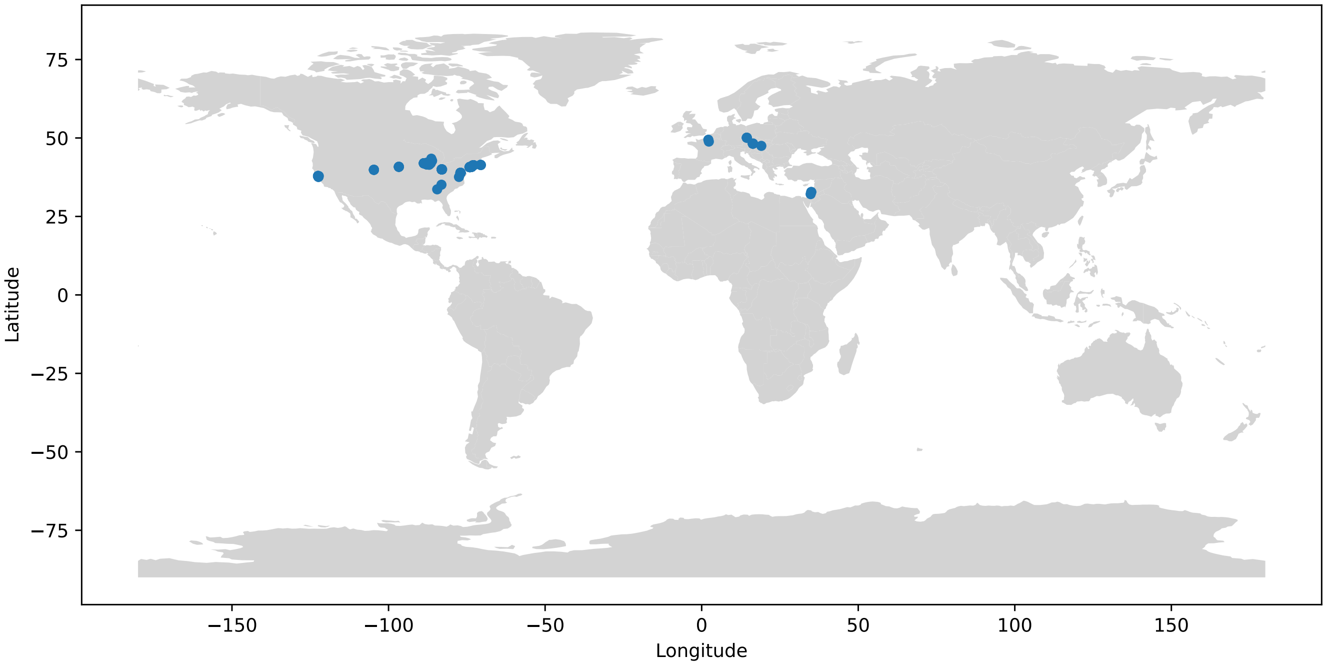

Figure 2: A world map showing the locations of the QR codes from our dataset.