SAM
Rights & Liberties

YEMENI NUMBER DETECTOR APPLICATION AND PRIVACY VIOLATION

February 2023

www.samrl.org

YEMENI NUMBER DETECTOR APPLICATION AND PRIVACY VIOLATION

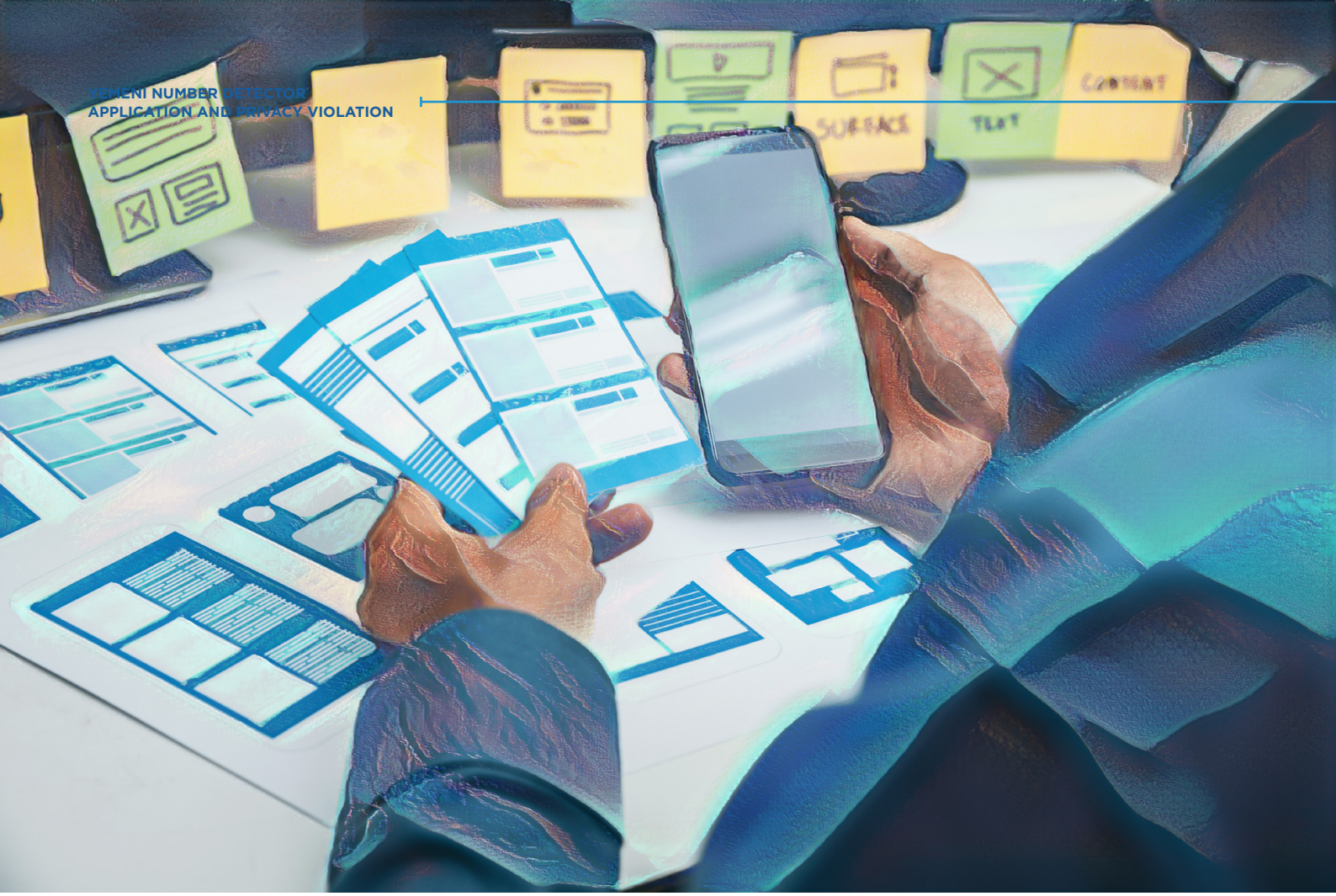
February 2023

SAM
Rights & Liberties

Digital Rights Project

A non-profit human rights window affiliated with SAM Organization, with the support of Internews, aims to introduce digital rights and monitor digital violations against users of the digital space, as it works to advocate for the digital rights of Yemenis, with the aim of reaching a safe, fair and free digital space. The window allows reporting digital violations, documenting them and creating a database about them. She publishes studies and research on digital activism, digital rights and digital security, in addition to planning and managing local and international advocacy campaigns.

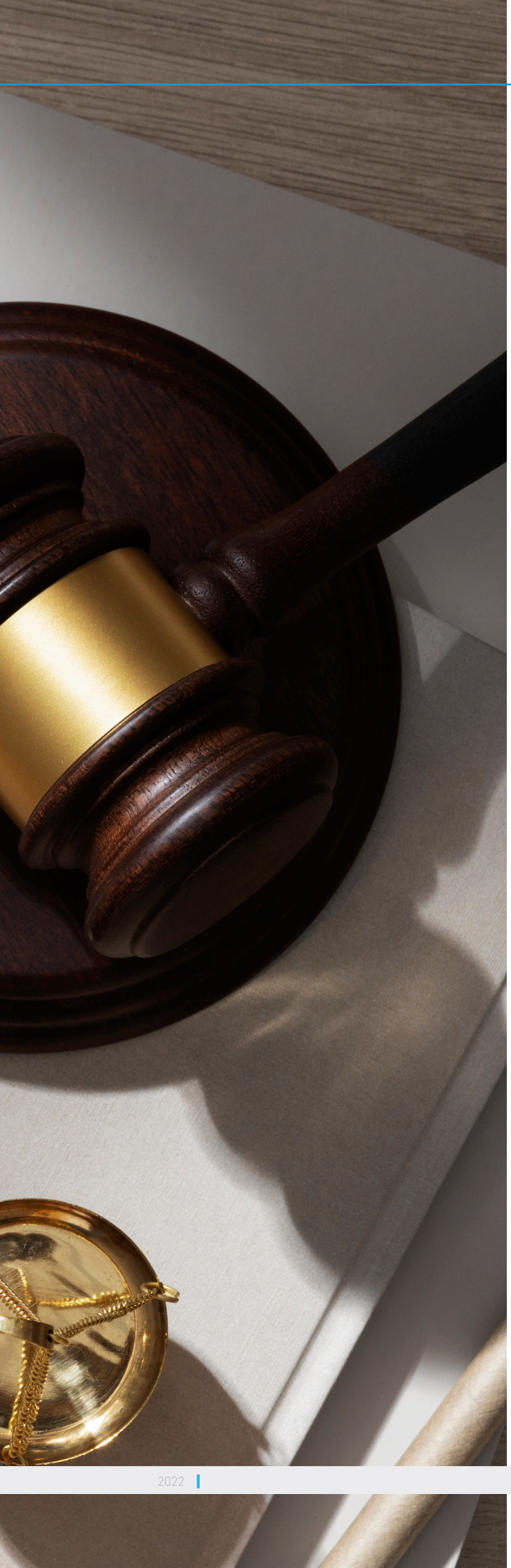
violations@samrl.org



Introduction

The «Yemeni Number Detector» application has gained immense popularity recently, as it is used by more than 5 million people, without realizing the risks and serious concerns it raises, regarding the privacy of users and the security of their data, as the application collects a large amount of personal information, including phone numbers, contacts and other sensitive information, which can be used for malicious purposes.

As the app continues to be promoted, it is important to assess its privacy practices and raise awareness among users about the risks associated with its use, which is what this report aims to do, which highlights those risks and makes recommendations to avoid, or at least mitigate them.



Legal context

Yemen is one of the countries that lack a privacy and data protection law, however, there are legal texts that have addressed the subject of privacy and data protection, as articles (from Article 44 to Article 57) of Draft Law No. (13) of 2012 on the right to access information (not implemented) stipulate the following:

Article (45): It is not permissible to argue the inadequacy or absence of information security systems to justify an illegal act that would harm the information.

Article (47): Each of the information systems used by the authorities must have the ability to verify and prove the responsibility of the actions in entering, processing, preserving, and retrieving information and access to the system and all the data contained therein.

Article (50): No party may collect, process, save, or use the personal data of the citizen, contrary to the Constitution and the laws in force.

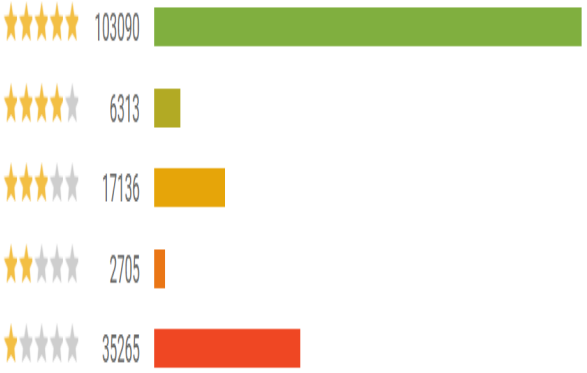
Article (52): The entity that holds personal data may not publish this personal data or give it to a third party except with the written consent of the person to whom this data relates.

Article (56): Each entity that keeps personal data shall be fully responsible for the protection of such data and shall develop an approved privacy statement showing the systems and procedures for dealing with the confidentiality of personal data and shall be available for viewing.

General framework

We could not find any information that leads us to know who is behind the application, and it seems that the anonymous developer (Pandora Soft) has realized early on the extent of the risks associated with the application, and the magnitude of the disasters it will cause, and therefore anonymity - he believes - exempts him from any obligation or legal accountability.

Nothing is obvious but ambiguity, no address, entity, or contact details exist, and their website



Feb 12, 2023	INSTALLS	5,000,000+ installs
Feb 4, 2021	INSTALLS	1,000,000+ installs
Jul 27, 2020	INSTALLS	500,000+ installs
Jan 27, 2020	INSTALLS	100,000+ installs
Dec 16, 2019	INSTALLS	50,000+ installs
Sep 23, 2019	INSTALLS	10,000+ installs
Sep 9, 2019	INSTALLS	5,000+ installs
Jul 14, 2019	INSTALLS	1,000+ installs
Jul 5, 2019	INSTALLS	500+ installs
Jun 26, 2019	NEW APP	Version 4.0 in TOOLS

have nothing but a "Privacy Policy" section. In addition, we contacted them more than once via the email listed on the site, to get answers to our questions, but we did not receive any response.

Since the announcement of the application in June 2019 until February 2021, the total downloads of the application reached more than one million downloads, and within two years, that is, until February 2023, the number of downloads increased to more than 5 million downloads, and the number of positive reviews from the "five-star" category that the application received, amounted to more than 100,000 reviews out of 166,000 reviews, according to statistics from AppBrain (a company that provides information about Android applications).

These figures indicate that the majority of users are not fully aware of the potential risks associated with using this application. Either due to a lack of education or their inability to access resources that can provide them with the information necessary to make mature decisions about the use of such applications, moreover, the fact that the application is popular with its risks may indicate a lack of interest or disregard for privacy and personal security by users.

How the application works

Although the app emphasizes that the subscriber's data is not shared with a third party, the idea of its work is to share the data it has taken from everyone - with everyone... [In this context] an expert in software and cybersecurity working in a UN organization (who stressed anonymity and his employer) explained to Online Source that those in charge of the application did not make any technical or professional effort to mitigate its major shortcomings, and all they did was to steal data from people's phones and add it to a database and make it available for publication without the slightest review, in an act he considered "intentional" to reap more profits and exploit people's lack of awareness of the issue of privacy. (Online Source - May 2022)

Information technology expert Dr. Ali Al-Saghir said in a statement to "Post Website" that the application does not derive its information from users' phones only, but also obtains it from Yemeni telecommunications companies, which he confirms are easily hacked due to the absence of government control over them and the lack of legal legislation obliging them to maintain the privacy of user data. (Post - December 2021)

Journalist Sami Noman believes in a Facebook post (May 2022) that the belief of some that the Yemeni number detector application, like any other application that takes names after the user's consent and permission to do so, involves ignorance or a defective failure to understand the issue of privacy, continuing: It is true that many applications request access to phone history, photos, and names, but you will not find an application that has 1% of the standards of respect that goes to publish it and makes it available to everyone without the slightest review, verification or restrictions, and the greatest ignorance In this aspect, the user's authorization only allows him to publish the number of the person to whom he subscribed and was allowed, not the numbers of the people registered on his phone.

Privacy Policy and User Rights

In an exclusive interview with the Digital Rights Project, a data security specialist (who asked not to be named) pointed out that "there are many gaps and potential risks in the privacy policy of the Yemeni Number Detector, with regard to the collection of user contact list information, including names and phone numbers. The privacy policy also does not specify what the app will do with this information and how it processes it and the developers have not stated how long users' data will be kept. As for third-party services, the Privacy Policy indicates that the application uses third-party services that may collect information to identify the user. However, it does not specify which third-party services are used or how they use the information collected.

"The privacy policy specifies that the app collects log data including a user's IP address, device name and operating system version, and therefore this information can be used to track users' online activities, which can be a privacy concern."

"The privacy policy clearly states that developers cannot guarantee the absolute security of users' data, which means that users' personal information may be at risk of being hacked or leaked," he said. "The privacy policy also lacks transparency, as it does not provide detailed information about the data collection and usage practices of the application, which may make it difficult for users to fully understand the risks and potential consequences of using the application," according to the data security specialist.

Chapter 3 of the General Data Protection Regulation (GDPR) (issued by the European Union in May 2018) sets out data privacy rights and principles that digital service providers should observe, in this regard, such as providing users with transparent and explicit information to understand how developers collect their data and the purpose for which it is used, the length of time in which the data is kept, as well as enabling them to exercise various rights including (the right to object to the processing of their data, and the right to erase and delete any information about them).

If we take these criteria, we find that the application of the "Yemeni Number Detector" does not guarantee any right to the user, for example, the application does not allow users to delete and erase data from their database, at all, even if the user deletes the application from his device, his data and the data of others (his contacts) remain stored on the application, which is a flagrant violation of everyone's rights.

Activist Majid Zayed, in a post on his Facebook page (August 2022), believes that what is crazy is the ease of adding to this application, offset by the difficulty of deleting and getting rid of bad names and fake and inappropriate descriptions, if a person wants to delete one name, he will wait a full day, after the application forces him to watch one or two mandatory ads of twenty seconds, and on the other hand, the application will not allow you to search for the name itself unless you give him the right to add a complete list of your contacts names.

The opportunism and deception are also manifested in the application developers asking users to subscribe to another application "International Number Detector" to be able to remove offensive numbers, according to the developers, and if the user subscribes to the new application, he will not be able to remove the offensive numbers in any case.

Privacy risks

Since the application has full access to the network, it is likely to monitor and collect sensitive user data such as login credentials, personal information, and browsing history, and the application can also access and collect user contact information, which may include sensitive data such as phone numbers, email addresses, and home addresses, and granting these permissions may also make the device vulnerable to security threats such as malware, viruses, and hacker attacks.

The application, its policies, and its service are a flagrant violation of all user privacy and various data, according to Adnan Othman, a web developer, and digital security researcher, who spoke to "Khoyout", saying: "Once (the Yemeni number detector) stores the data of only one user once installed, then it has stored the data of hundreds of other users registered in the name register saved with it, and not only the username register but in addition, their emails and other account addresses associated with the name register." Othman stresses that the worst threat is the sharing of name records with third parties,

using the app's data search engine, saying: "This unspoken vulnerability is, in fact, backward and will have various tragic consequences, including violence, disputes, and family problems, because many users trust these results completely, without any doubt."

Information technology researcher Aseel Abdul Mughni revealed a vulnerability in the "Yemeni Number Detector" application that attackers could exploit to access the bank accounts of users who save the bank account number and password of contacts.

Researcher Abdul Mughni explained to the Digital Rights Project the details of the vulnerability, which already shows how dangerous it is for all of you to know that applications that do not use strong security protocols and do not follow security best practices can be exposed to hacker attacks and hacks. Although we can't predict the severity of this vulnerability in the app, using untrusted apps may put you at risk.

Information technology expert Dr. Ali Al-Saghir said in a statement to "The Post" that number detection applications in Yemen have become a haunting problem because they violate the privacy of users... Al-Saghir believes that the absence of a cybercrime law exposes Yemeni users to digital penetration in the absence of government oversight of the digital reality in the country. (Post - December 2021)

Researcher and legal advisor Abdulrahman Al-Zabib mentioned in an interview with Al Hawyah Channel (dated June 2022)

The failure of the company that owns the application to comply with the informed consent of individuals that all contact numbers saved in the phone will be revealed and published. It is considered a crime of assault on the privacy of individuals and society according to Yemeni law, adding that the application poses risks to national security, as it allows any person or entity in any country in the world to withdraw the database of phone numbers of Yemeni citizens through the number detector application.

Catastrophic consequences

The risks of the application do not stop at the limit of revealing users' data and violating their privacy, but extend beyond that, and include all personal, social, and psychological aspects, and the risks are not limited to its users only, but also affect people who are not involved in it, in a violation that includes everyone.

In this context, journalist Sami Noman - a previous source - asks: Who gave the application the right first to publish my name and number with shameful and fake descriptions? Who gave them the right to publish, falsify, violate my privacy, and reveal my true identity to others, while I did not subscribe to the application, he continues: ... If the telecommunications companies do not allow revealing the identity of a single subscriber - even if I come to them and prove to them that he is an annoying person - except by order of the prosecution or at least Search and police, then this anonymous app comes to display names in this reprehensible way.

Dr. Samia Al-Aghbari, Assistant Professor and Head of the Department of Journalism at Sana'a University, and a feminist activist against violence against women consider the application of "Number Detector" as an invasion of privacy in general, and of women in particular, and that it will increase the intensity of violence against women - and as a result - they will lose their freedom completely. Al-Aghbari adds to "Khoyout" that the double and complex relationship between such electronic phenomena on the one hand and the law on the other is in itself part of the dilemma and gap in that application. (Khoyout Platform - April 2022)

Activist Majid Zayed believes that this application offers millions of people of all categories the possibility of distortion, defamation, blackmail, exploitation, and directing descriptions and names based on prior and deliberate intentions... This simplicity in the process of adding made the application a tempting way in the hands of psychopaths, tendentious and plagued by doubts and disorder to harm those who want, as he described.

Al-Saghir says that the danger of digitizer applications lies in the possibility of using users' data for political purposes that may harm them or selling it to other dangerous parties or applications, in addition to their ability to exploit that data to achieve advertising or commercial purposes at the expense of people. (Post - December 2021)

It is worth saying that it is not excluded that the application will be hacked and then user data will be displayed in auctions, as is the case with the global Truecaller application, according to the American company Cyble (a provider of dark web threat intelligence), the data of 47.5 million users of the Indian Truecaller application was sold on the dark web, for only $ 1,000. (Cyble – May 202), and in May 2019, a cybersecurity researcher reported that data from 300 million Indians using the Truecaller app was offered for sale on the dark web. The leaked data included mobile phone numbers and, in some cases, email addresses, photos, company names, job titles, and more. (Bank Info Security - May 2019).

The role of official institutions

In August 2022, activists launched a campaign against the number detector application and the damage and problems it caused to many women, and they called on the Ministry of Communications to ban this application and all number detection applications.

In an implicit response to the reactions, the Minister of Communications in the Sana'a government, Eng. Misfer Al-Numeer, stated in a tweet on Twitter (August 2022), saying: The Ministry of Communications and Information Technology work in accordance with the laws and regulations of its organization, calling on those who have a complaint of harm (affecting him or society) on an application or website to submit his complaint officially to the ministry, and the ministry will not hesitate to study complaints and take the necessary action in accordance with the law, as he put it.

In turn, Yemeni telecommunications companies sent SMS messages to users in May and November 2022, warning them against downloading and using number detection applications, to ensure the protection of user privacy and phone data.

An official in the Public Telecommunications Corporation (who preferred not to be named because he is not authorized to talk), explained to Al-Masdar Online that this application is linked to the Google Store and not a website that can be blocked, which requires following other procedures that do not pass through the Corporation. The names displayed in the Yemeni number detector app are random and fake, and have nothing to do with telecommunications companies from near or far, he said, but are "stolen" from subscribers' phones. (Al-Masdar Online - Previous Source)

What should be done?

Information technology expert Dr. Ali Al-Saghir confirms that the issue of banning "number detection programs" requires government communication to sites that provide the ability to download them, such as Google Play and others, and the need to legislate digital security laws to pressure transcontinental companies to adhere to the privacy of information security in the country, but this is far from being achieved in light of the state of collapse that the Yemeni state is going through and the ongoing war in the country. To avoid falling into the risks of digital security, Al-Saghir recommends the need to delete number detection applications and all harmful applications from phones and computers and be careful not to bear them at all, calling for work to spread community awareness among people about the danger of some applications. (Post-Previous source)

The activist "Majid Zayed" – a previous source – adds: If the state does not perform its duty towards it, and towards its transgressions and damages, it is our right as a society to confront the application and show its dangers and the many tragedies and damages it caused, and we also have the right to call on the public to report it, boycott it, and mobilize to remove it from users' devices, according to moral, human rights and legal motives and definitely the ways of the malicious in our Yemeni society in particular.

IT researcher Aseel Abdul Mughni advises to stop using the application immediately, start changing the passwords for the accounts that have been saved within the contact, as well as change the password for the bank account, and notify the bank of any unauthorized changes in the customer's account.

Conclusion

While the number detector application may seem serviceable, it carries many risks for users, and non-users, which makes it imperative for individuals to be aware of these risks and take steps to protect their personal information and privacy online. Moreover, the app highlights the need for more education and awareness about the risks associated with using such apps.


SAM
Rights & Liberties

YEMENI NUMBER DETECTOR APPLICATION AND PRIVACY VIOLATION

February 2023

violations@samrl.org
www.dg.samrl.org

Digital.Rights.Yemen
@SamDigitalRight

SAM
Rights & Liberties

www.samrl.org
info@samrl.org