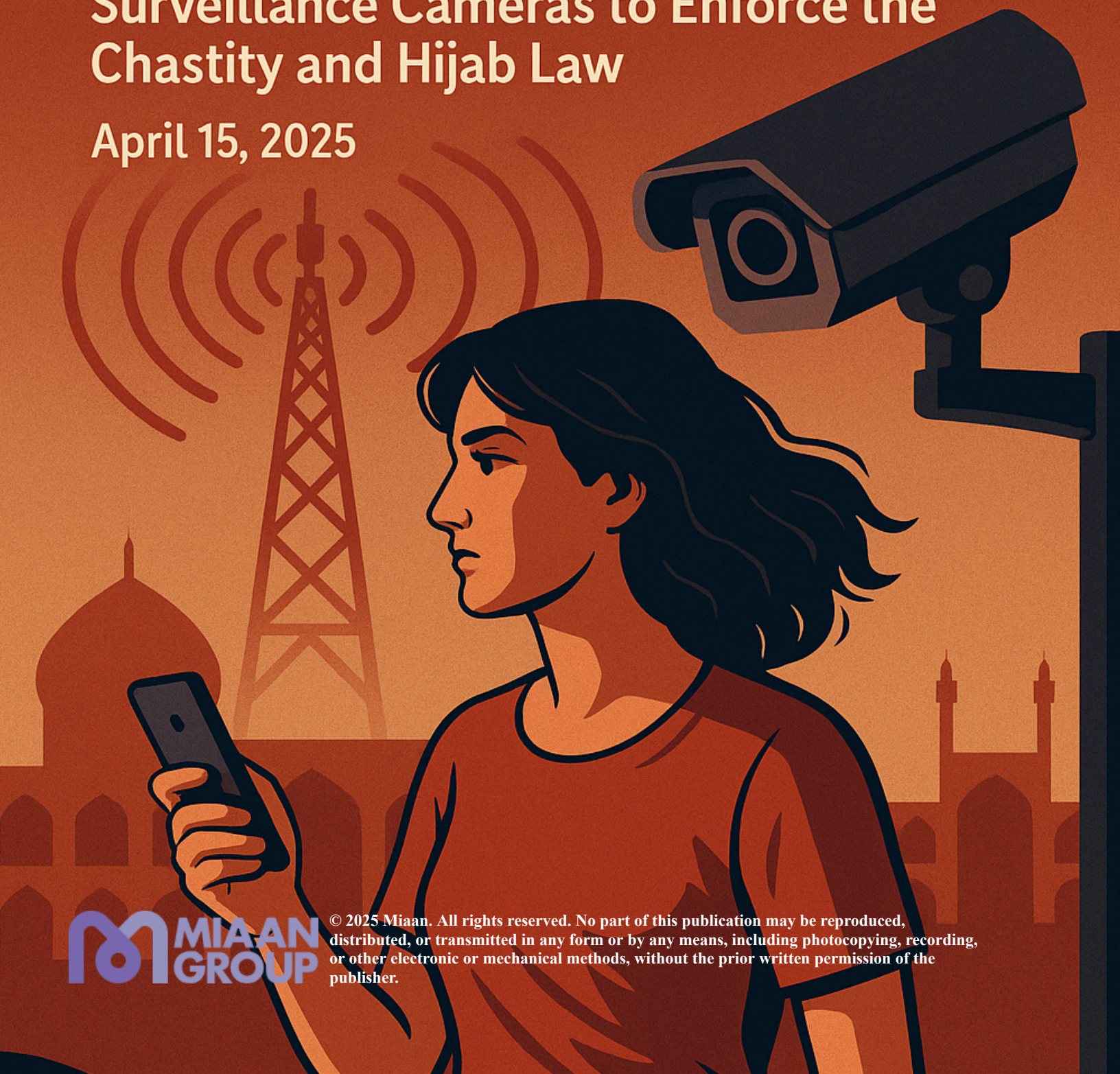
A BATTLEFIELD NAMED ISFAHAN

Targeted Use of IMSI-Catchers and Surveillance Cameras to Enforce the Chastity and Hijab Law

April 15, 2025



MIAAN GROUP

Executive Summary

Iran's Chastity and Hijab law—and the social backlash it has provoked, particularly following the death of Mahsa (Zhina) Amini—has prompted intensified government efforts to control women's clothing. Although the law was officially shelved, at least temporarily, following a decision by the Supreme National Security Council in December, evidence suggests that aspects of it are still being implemented on a limited and regional basis. In this context, the city of Isfahan has become a prominent example of deploying advanced surveillance technologies to identify and intimidate women who refuse to wear the compulsory hijab.

This report details a multilayered system designed to suppress women's right to choose their dress through technological means. It further explains how tools such as International Mobile Subscriber Identity-Catchers (IMSI-Catchers), contactless card readers, and surveillance cameras are used in Isfahan to systematically violate women's rights, especially the rights to privacy, freedom of expression, and non-discrimination.

Reports from Isfahan present an alarming picture of the targeted and systematic use of surveillance technologies to control women's bodies and enforce mandatory hijab laws. The combined use of IMSI-Catchers, contactless card readers, and surveillance cameras—along with access to government databases and the cooperation of telecom operators—has created a powerful, multilayered tool to systematically violate women's rights through identification, tracking, and intimidation of those who choose voluntary dress.

To investigate this operation in Isfahan, Filterwatch interviewed nearly twenty individuals who had received threatening text messages and those with access to sufficient evidence about the implementation of the plan due to their employment in institutions and companies involved in

the operation. The identities of all these individuals will remain confidential to ensure their safety.

Filterwatch's investigations reveal that the crackdown on women without mandatory hijab in Isfahan is being carried out through coordination among several law enforcement, security, judicial, and even cultural institutions.

This project not only constitutes a serious violation of fundamental women's rights—including the right to privacy, the freedom to choose how to dress, and freedom from discrimination—but also signals the normalization of using invasive surveillance tools for social engineering and the suppression of any civil disobedience.

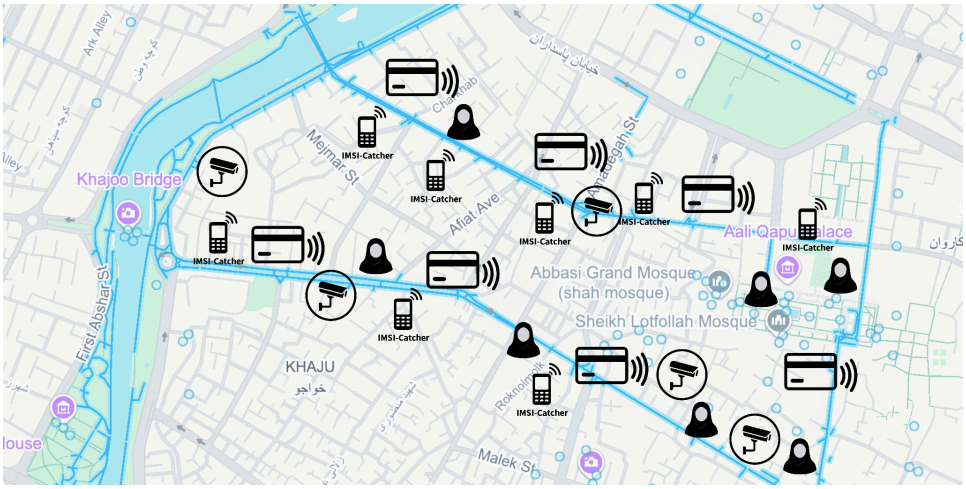
The transformation of everyday tools—like mobile phones and ID cards—into instruments of social control represents a dangerous and escalating trend that severely threatens individual freedoms. The Isfahan case is a serious warning about the intensification of digital authoritarianism and the use of technology as a weapon against citizens' rights, especially those of women, in Iran.

The Multi-Layered Technology in Use

This system is based on the combination of three technologies:

1. **International Mobile Subscriber Identity-Catchers (IMSI-Catchers):** These devices operate by impersonating telecom towers and can capture the unique IMSI (International Mobile Subscriber Identity) of mobile phones within their range. Our studies indicate that an area between 30 to 35 square kilometers in central Isfahan (especially tourist areas) is covered by these devices.

How it works: These devices impersonate legitimate telecom towers (BTS). Phones within range connect to the fake tower due to its stronger signal. Upon connection, the device requests and records the SIM card's unique IMSI. Some devices may also collect IMEI (International Mobile Equipment Identity). This method exploits a security vulnerability in GSM networks, where the network is not required to authenticate itself to the mobile phone. More advanced devices may force phones to downgrade from 3G/4G/5G to 2G to facilitate the attack. Victims of this system may experience temporary disruptions in phone calls or internet access.



A schematic map of the surveillance tools used in Isfahan's tourist area based on witness information shared with Filterwatch

The history of state control over Iran's telecommunications and systems like "SIAM," a web program for remotely manipulating cellular connections, developed by the Communications Regulatory Authority, has the technical ability to force network downgrades from 3G/4G/5G to 2G, which is required for such attacks.

One woman who received such a threatening SMS told Filterwatch that minutes before receiving the message, she was on a WhatsApp call that was suddenly cut off and she lost access to the internet—although she regained it shortly after receiving the message.

Another person who was uploading a photo on Instagram in the Naqsh-e Jahan Square (also known as the Imam Square) area told Filterwatch that they experienced a brief disruption, which ended after receiving a message from the "Promotion of Virtue and Prevention of Vice" headquarters.

They told Filterwatch they didn't check whether their internet had dropped from 3G/4G/5G to 2G, but the momentary loss of internet could be a sign of such downgrading.

These devices have been deployed in several forms:

- **Portable:** With a reported range of 100 to 500 meters, used by officers (likely from the Promotion of Virtue staff) to patrol and get close to targeted women to record their IMSI.
- **Vehicle-based:** With a reported range of 1 to 2 kilometers.
- **Stationary:** With a reported range of up to 5 kilometers, likely used for permanent monitoring of key areas.

The use of portable, vehicle-based, and stationary IMSI-Catchers with different ranges indicates a complex, layered strategy for tracking. Portable units allow targeted tracking in pedestrian-dense areas (like Naqsh-e Jahan Square), vehicle units cover wider street zones, and stationary units provide continuous monitoring of key zones.

2. **Contactless Card Readers:** These devices use RFID or NFC technology to read the data stored on smart national ID cards or metro cards. The primary aim is to obtain the person's national ID number. A critical point is that these devices have a very short range (less than one meter), requiring officers to be physically very close to targeted women to read their card data. The report claims about 50 square kilometers of the city are covered by agents equipped with these readers.

3. **Urban Surveillance Cameras (CCTV):** Footage from certain urban cameras is monitored by operators from the police's "Prevention" and "Cyber Police" units. If a woman is spotted violating the mandatory dress code, her location is texted to field agents equipped with IMSI-Catchers or card readers to be dispatched for identification. This indicates integration between existing surveillance systems and mobile tracking teams. This contradicts the statement of Mohsen Mazaheri, head of the Promotion of Virtue headquarters in Isfahan, who denied the use of urban surveillance cameras in this process. However, the general trend of increased electronic surveillance (including drones and facial recognition) for hijab enforcement in Iran has been confirmed by UN reports.

Identification Process: From Raw Data to Personal Identity

The main challenge of this system is converting raw identifiers (IMSI or national ID numbers) into actionable identity information for sending threatening SMS messages. Technical analysis shows this is done through two primary mechanisms:

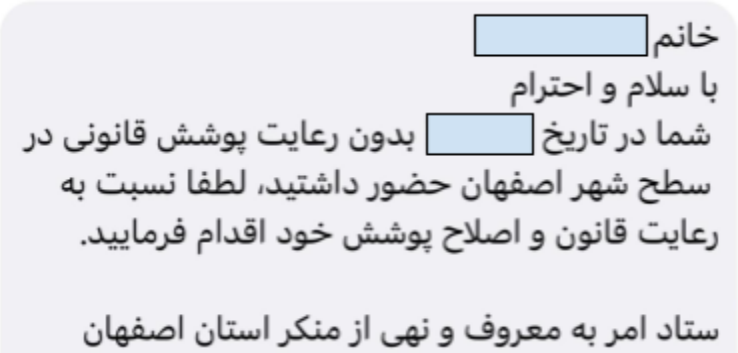
1. **Cooperation with Mobile Operators:** To convert recorded IMSI into phone numbers and subscriber details, cooperation with mobile operators is essential.
2. **Access to Government Databases:** The national ID number obtained through card readers is used to query official databases such as the Civil Registration Office, police, and the Comprehensive Identity System to retrieve the person's name, father's name, and registered phone numbers. The report's mention of "father's name" strongly suggests the use of the Civil Registration database.

This data linkage process, likely automated or semi-automated to justify the reported speed (such as sending messages in under 15 minutes), heavily relies on centralized governmental data infrastructure and legal or practical access to operator information.

Law Enforcement Through Intimidation: Threatening SMS Messages

The end product of this surveillance system is the sending of threatening SMS messages to identified women. These messages, examples of which appear in this report, are typically sent by the “Promotion of Virtue and Prevention of Vice” headquarters and ask the individual to “correct” their clothing. Mohsen Mazaheri, the head of this headquarters in Isfahan, has confirmed the sending of 97,500 “hijab warning” messages.

One recipient told Filterwatch that during the Nowruz holidays, less than 15 minutes after walking in Naqsh-e Jahan Square (Imam Khomeini) with a scarf around her neck, she received a threatening message from the headquarters.

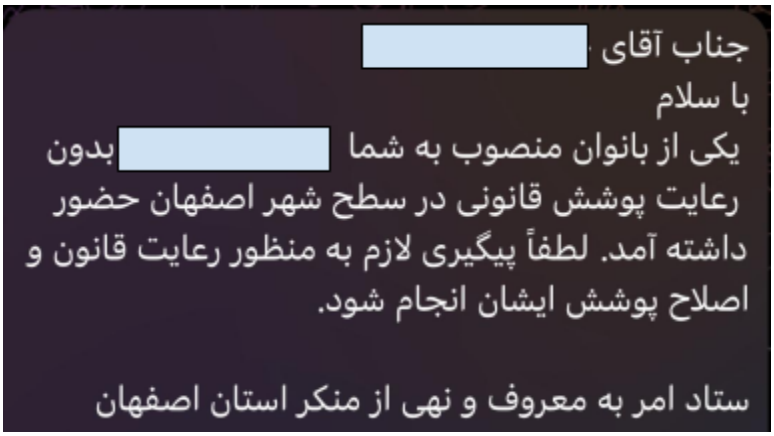

خانم [redacted]
با سلام و احترام
شما در تاریخ [redacted] بدون رعایت پوشش قانونی در سطح شهر اصفهان حضور داشتید، لطفا نسبت به رعایت قانون و اصلاح پوشش خود اقدام فرمایید.

ستاد امر به معروف و نهی از منکر استان اصفهان

An image of the SMS sent to a female citizen, shared with Filterwatch for publication

More worryingly, reports and testimonies indicate that these messages are sent not only to the individual but also to her family members (father, brother, husband). The head of the Isfahan Promotion of Virtue headquarters justified this by citing “the need for educational awareness” and “informing families,” but did not explain how family information is obtained or why pressure is being placed on families. The example of a citizen whose ID card was with his sister and who received a threatening SMS highlights both the potential for system errors and the intention to involve families.

A male citizen of Isfahan told Filterwatch: “I had given my national ID card to one of my sisters for some administrative work, and an hour later I received a message asking me to take action regarding correcting her dress.”



An image of the SMS sent to a male citizen, shared with Filterwatch for publication

Amirhossein Bankipour, member of the Cultural Commission of the Parliament, who is one of the main architects of the "Chastity and Hijab Law," confirmed the implementation of this plan in Isfahan, claimed its success and announced plans to expand it to other cities.

"It started a long time ago, and its effects were also observed. Almost 80 to 90 percent of those who received the text message complied. This is a very good approach that does not create social tension either," said Amirhossein Bankipour on April 9 2025, regarding the pilot implementation of this plan in the city of Isfahan.

In recent weeks, various institutions and individuals have pressured the 14th government to implement the Chastity and Hijab Law. This includes gatherings of compulsory hijab supporters in front of the parliament and in the city of Qom. However, according to Nabavian, one of the law’s drafters and ratifiers, due to the rapid fall of Bashar al-Assad in Syria and to avoid what he called the “Syria-ization” of Iran, the law has not been “officially” announced by the Supreme National Security Council. Nevertheless, extensive evidence—including the crackdown on

unveiled women in Isfahan and the "Nazer" app—indicates that at least parts of the law are being implemented on a limited and regional basis.

Detection and Defending

International Mobile Subscriber Identity-Catchers, abbreviated as IMSI-Catchers, are electronic surveillance tools designed to track and intercept mobile phone communications. These devices are also known by other names such as Stingray, Cell Site Simulator (CSS), fake cell tower, rogue base station, or drop boxes. The International Mobile Subscriber Identity (IMSI) is a unique number that identifies each mobile device to the network operator.

However, users can significantly reduce the risk by adopting a series of measures. These measures include disabling 2G connectivity on the device (if possible), extensive use of end-to-end encrypted (E2EE) communication apps to protect content, using a VPN for internet traffic, keeping device software updated, and smart use of airplane mode or Faraday bags in sensitive situations. It should be emphasized that achieving complete protection for ordinary users is currently not feasible, and the primary goal should be to reduce risk and increase the cost and complexity for attackers. The role of network operators in implementing advanced security features and monitoring the network is critical, although progress in this area (such as with 5G SA) is slow and faces challenges.

Based on the presented analysis and considering the limitations, the following practical recommendations are offered to increase users' resilience against IMSI-Catchers:

1. **Disabling 2G connectivity:** This is the most effective single technical measure against the most common methods of content interception. If your Android device allows it (via

network settings or the *##4636##* code), disable 2G connectivity. Be aware of potential impacts on coverage in certain areas.

2. **Using E2EE communication apps:** For all sensitive conversations (messages and calls), use apps like Signal instead of standard SMS and phone calls. Keep in mind that this primarily protects the content, not necessarily all metadata.
3. **Using a reliable VPN:** For internet browsing, especially on untrusted networks or if concerned about cellular data interception, use a reputable and trustworthy VPN service or Tor.
4. **Awareness of network anomalies:** Pay attention to unexpected changes such as frequent downgrades to 2G, persistent connection issues, or rapid battery drain—especially in unusual circumstances. Consider these as potential warnings, not definitive proof.
5. **Using airplane mode or Faraday bags:** In highly sensitive locations or when complete disconnection is desired and feasible, use airplane mode or, for extra assurance, a Faraday bag.
6. **Keeping your device updated:** Install OS and app updates promptly to benefit from the latest security patches.
7. **IMSI-Catcher detection apps:** Use Android detection apps like Android IMSI-Catcher Detector (AIMSICD), SnoopSnitch, Sitch, GSM Spy Finder, Cell Spy Catcher with great caution and full awareness of their significant limitations (including the need for root access or specific chipsets) and high likelihood of false results. Do not rely on them for guaranteed security. It may even be better to refrain from strongly recommending their use due to the risk of creating a false sense of security. Users must have precise and accurate technical knowledge to effectively use such tools, and if such knowledge is lacking, their use is not recommended.
8. **Understanding metadata risks:** Be aware that even with E2EE and VPN use, some communication metadata (such as time, volume, and communication parties) may still be observable.