You Move, They Follow

Uncovering Iran's Mobile Legal Intercept System

By Gary Miller (https://citizenlab.ca/author/garymiller/), Noura Al-Jizawi (https://citizenlab.ca/author/noura/), Ksenia Ermoshina (https://citizenlab.ca/author/kermoshina/), Marcus Michaelsen (https://citizenlab.ca/author/mmichaelsen/), Zoe Panday (https://citizenlab.ca/author/zpanday/), Genny Plumptre (https://citizenlab.ca/author/gplumptre/), Adam Senft (https://citizenlab.ca/author/adamsenft/), and Ron Deibert (https://citizenlab.ca/author/profd/)

January 16, 2023

A confidential source sent the online news organization, *The Intercept*, a series of internal documents and communications providing details on what appear to be plans to develop and launch an Iranian mobile network, including subscriber management operations and services, and integration with a legal intercept solution. Some of this communication included representatives of the Communications Regulatory Authority of Iran (CRA). In October 2022, *The Intercept* shared this material with Citizen Lab researchers for analysis. The following report provides a summary of our analysis of this material and discusses its wider implications.

Key Findings

- Iran CRA regulations state that all telecom operators in Iran must provide the CRA with direct access to their system for retrieving user information and changing their services. Justified under its own broadly defined "Legal Intercept" provisions, the CRA aims to use this sophisticated system to store user information, allow or deny a user's access to mobile services, and view historical voice, SMS, and data usage.
- The CRA's Legal Intercept system uses APIs to integrate directly into mobile service providers' operational systems, including acquiring detailed data on service ordering, service fulfillment, and billing history stored in the service provider data warehouse. Any new, termination, or change request for a user's SIM card must be validated by the CRA, using the API from the mobile provider to request approval from the CRA prior to enacting the change.
- This type of state-sponsored system used to directly manage the operations of independent mobile networks in a country is extremely rare in the modern mobile communications industry. If implemented fully as envisioned in the documents we reviewed, it would enable state authorities to directly monitor, intercept, redirect, degrade or deny all Iranians' mobile communications, including those who are presently challenging the regime.

- Documents indicate that firms based in Russia, the United Kingdom (UK), and Canada engaged in extensive discussions to provide commercial services and technology to support Iran's Legal Intercept requirements of mobile surveillance, service control, and account management. While the documents we reviewed did not include fully executed agreements, the negotiations among the key stakeholders were advanced and revealed extensive details about Iran's legal intercept system and the type of services and technologies that would be provisioned from the private sector to support it.
- A list of all documents we reviewed, and their timeframe, is included in Appendix A.

Background on Iran, Information Controls, and Democratic Protests

Iran's recent history has been marked by repeated periods of political contestation. These include (https://time.com/6234429/iran-protests-revolution-history/) the student protests (https://www.nytimes.com/1999/07/11/world/student-protests-shake-iran-s-government.html) of 1999, the 2009 Green Movement (https://iranprimer.usip.org/resource/green-movement), and protests over the country's socio-economic situation in 2017/2018 (https://www.brookings.edu/research/the-islamic-republic-of-iran-four-decades-on-the-2017-18-protests-amid-a-triple-crisis/) and 2021 (https://www.nytimes.com/2021/11/26/world/middleeast/iran-protests-water-shortages.html). The September 2022 (https://www.bbc.com/news/world-middle-east-62930425) protests, which erupted after Mahsa Jina Amini, a 22-year-old Kurdish woman, was beaten to death in the custody of the morality police for allegedly violating strict *hijab* rules, are the latest manifestation in a long struggle (https://newlinesmag.com/argument/a-new-iran-has-been-born-a-global-iran/) for political rights and social justice.

The Iranian regime has responded to such protests (https://www.hrw.org/news/2022/10/05/iran-security-forces-fire-kill-protesters) with severe crackdowns and countless human rights abuses, including (https://www.ohchr.org/en/press-briefing-notes/2022/11/iran-critical-situation) through (https://www.amnesty.org/en/location/middle-east-and-north-africa/iran/report-iran/) arbitrary detentions, forced disappearances, gender-based and sexual-based violence, executions, and denying detainees a fair trial. Women (https://www.ohchr.org/en/press-releases/2021/03/iran-women-and-girls-treated-second-class-citizens-reforms-urgently-needed), the LGBTQ+ (https://www.amnesty.org/en/documents/mde13/4129/2021/en/?utm_source=annual_report&utm_medium=epub&utm_campaign=2021&utm_term=english) community, and religious and ethnic minorities suffer systemic discrimination (https://www.hrw.org/world-report/2021/country-chapters/iran#814a01). In November 2022, the estimated death toll during (https://www.ohchr.org/en/news/2022/11/high-commissioner-human-rights-councils-special-session-iran-must-stop-violence) the fall 2022 protests reportedly (https://www.iranintl.com/en/202212216716) stood at over 300 people, along with over 14,000 people being arrested and some sentenced to death (in December 2022, another Iranian human rights organization based in the United States reported over 500 dead and over 18,000 arrested). Security forces have used indiscriminate shooting and live bullets against peaceful demonstrators. In short, Iran's civil society, journalists, activists, and dissidents operate in a precarious and dangerous environment (https://volunteeractivists.nl/en/wp-content/uploads/2018/10/Civil-Society-in-Iran-and-its-Future-Prospects-pdf.pdf).

One prominent characteristic of the Iranian regime is the persistent violation of the rights to freedom of expression (https://digitallibrary.un.org/record/791024?ln=en), association and peaceful assembly (https://www.google.com/url?q=https://www.ohchr.org/en/documents/country-reports/a77181-situation-human-rights-islamic-republic-iran-report-special&sa=D&source=docs&ust=1671173899774402&usg=AOvVaw39WL6kOZwR4ixQqBq08gPR), freedom of thought, conscience, and religion (https://www.ohchr.org/en/press-releases/2022/08/iran-un-experts-alarmed-escalating-religious-persecution), and access to information (https://www.ohchr.org/en/press-briefing-notes/2021/07/access-reliable-information-sources-obvious-antidote-

disinformation#:~:text=The%20right%20to%20information%2C%20under,providing%20access%20to%20the%20Internet.). The Islamic Republic has sought to impose restrictive measures to control information and activities in the digital space in various ways, including online surveillance, censorship, cyber espionage, the adoption of information control legislation, and policing online discourse. Iran ranks 178 out of 180 countries on the 2022 World Press Freedom Index (https://rsf.org/en/country/iran) and is considered "not free" in Freedom House's 2022 Freedom on the Net (https://freedomhouse.org/country/iran/freedom-net/2022) report, which describes Internet freedom in the country as "highly restricted."

For example, Iran has institutionalized Internet censorship through various government bodies. The Supreme Council of Cyberspace (https://www.iranhumanrights.org/wp-content/uploads/EN-Guards-at-the-gate-High-quality.pdf), established in 2012 by order of the Supreme Leader, centralized decision-making over internet development and control under the direct authority of Ayatollah Khamenei. Other important institutions (https://www.iranhumanrights.org/wp-content/uploads/Internet_report-En.pdf) include the Working Group to Determine Criminal Content, responsible for identifying web content to be filtered, and the Iranian Cyber Police (FATA), established in 2011 to combat cybercrime and threats against national security. Alongside these bodies, the CRA, founded in 2003, regulates the communications sector, including broadcasting and telecommunications.

The regime employs a range of sophisticated information control measures aimed at influencing and restricting information access, shaping online content, and stifling dissent. At the center is the government-controlled intranet, the National Information Network (NIN), which is also known as SHOMA (https://www.wired.com/beyond-the-beyond/2019/11/iranian-national-cyberspace/) or "halal internet (https://rsf.org/en/iran-creates-halal-internet-control-online-information)." Launched in 2012 (https://www.jeuneafrique.com/174142/economie/avec-son-propre-internet-halal-l-iran-nettoie-la-toile/), the NIN project establishes and incentivizes the use of domestic internet infrastructures (https://www.article19.org/data/files/The_National_Internet_AR_KA_final.pdf), purportedly with the aim of improving bandwidth, deepening internet penetration, protecting information security, and impeding international surveillance. In reality, users are subject to systematic monitoring, content blocking, and filtering. Freedom on the Net (https://freedomhouse.org/country/iran/freedom-net/2022#footnote18_znou4h2) has reported that Iranian authorities are able to effectively block access to websites within a few hours. The result is Internet fragmentation (https://techpolicy.press/internet-shutdowns-and-censorship-in-iran-and-beyond/), as siloed local infrastructures permit government authorities to block access to the global Internet while maintaining local connectivity.

Recent legislation, in particular the so-called *User Protection Bill*, threatens to complete Iran's digital isolation. The highly controversial (https://www.ohchr.org/en/press-releases/2022/03/un-human-rights-experts-urge-iran-abandon-restrictive-internet-bill) bill (https://www.accessnow.org/iran-internet-bill/) aims to give the security forces control over Iran's Internet gateways, oblige foreign Internet services to follow the laws of the Islamic Republic, and criminalize the use of VPNs which enable Iranians to bypass censorship. The current administration seems to silently (https://www.article19.org/resources/iran-draconian-internet-bill/) enact these measures although the bill has never been ratified by parliament. As part of the implementation, the government uses methods of deep packet inspection to detect and disrupt (https://www.article19.org/resources/tightening-the-net-is-the-dangerous-user-protection-bill-still-imminent/) VPN connections in data traffic.

The Iranian authorities strategically use Internet shutdowns and disruption during elections (https://onlinelibrary.wiley.com/doi/full/10.1111/ropr.12333?casa_token=gTZ3X3tQS8YAAAAA%3AQqo8Ssl3MZamW0UXZK5i5UDwnEPKtKpYfrGl575Gbr46vT3CVPwglnRPVBFLtvX_qLJis5HOgmURIKQ#:~:text=https%3A//doi.org/10.1111/ropr.12333) and protests. For example, a nation-wide shutdown (https://www.article19.org/ttn-iran-november-shutdown/) was implemented in response to the November 2019 protests. During the 5-day blackout, security forces killed (https://iran-shutdown.amnesty.org/) an estimated number of up to 1,500 people. During and after the September 2022 protests, OONI (https://ooni.org/post/2022-iran-technical-multistakeholder-report/) reported a significant increase in Internet

censorship, including the blocking of commonly used applications such as Instagram, LinkedIn, WhatsApp, Skype, the Google and Apple app stores, and encrypted DNS. The authorities also implemented daily shutdowns to Irancell, Rightel, and MCCI, the country's top 3 mobile network providers.

Mobile Services in Iran are Far From Normal

The documents shared by *The Intercept* were a series of emails sent by representatives of the companies listed below, as well as documents attached to these emails (for a complete list of documents reviewed, see Appendix A). Citizen Lab researchers scanned the emails (https://github.com/ninoseki/eml_analyzer) to confirm the authenticity of the sender, recipients, content, body, and document attachments. Companies (and one agency) whose correspondences we reviewed include:

- **Ariantel** – An Iranian-based Mobile Virtual Network Operator (MVNO), the primary source of the emails.
- **Telinsol** – A UK-based satellite communications consultancy which appears, based on the documents we reviewed, to have conducted international business transactions with vendors on behalf of Ariantel.
- **PROTEI** – An international telecommunications systems vendor founded in Russia which was selected, as indicated in the documents reviewed, by Ariantel to provide core network components to the company in support of user authentication, data management and Deep Packet Inspection (DPI), SMS delivery, and mobile network signaling.
- **PortaOne** – A Canada-based mobile business and support system vendor, which was selected, as indicated in the documents reviewed, by Ariantel to provide mobile account creation, service provisioning, billing, and customized integration with Iran's Legal Intercept system.
- **Iran CRA** – Iran's Communication Regulatory Authority, which is tasked with executing governmental powers, supervision, and executive powers of Iran's Ministry of Information and Communication Technology.

The technical detail included in the documents sheds new light into the level of sophistication Iranian authorities sought to use to conduct surveillance operations and control access to mobile information and communications. The software and services offered by the vendors allows the CRA to integrate with mobile service provider systems used for billing, service activation, and management functions including a web service API called "SIAM" (https://theintercept.com/document/2022/10/28/irans-siam-manual-for-tracking-and-controlling-mobile-phones/). The email shown below, sent by the CRA's "Directorate General of Communications Systems Security," seems to indicate that Ariantel has deployed a fully operational mobile network in Iran, integrating with the CRA's Legal Intercept system, which has experienced a service interruption. Translated to English, it reads.

> Greetings and Regards
>
> The attached file containing Siam system documents was sent.
>
> It should be noted that due to the frequent and long interruption of your service, please take the necessary measures to solve the problem and ensure the durability of the service.
>
> Thanks
>
> Ali Safai
>
> Directorate General of Communication Systems Security

(https://citizenlab.ca/wp-content/webpc-passthru.php?src=https://citizenlab.ca/wp-content/uploads/2023/01/image4.jpg&nocache=1)

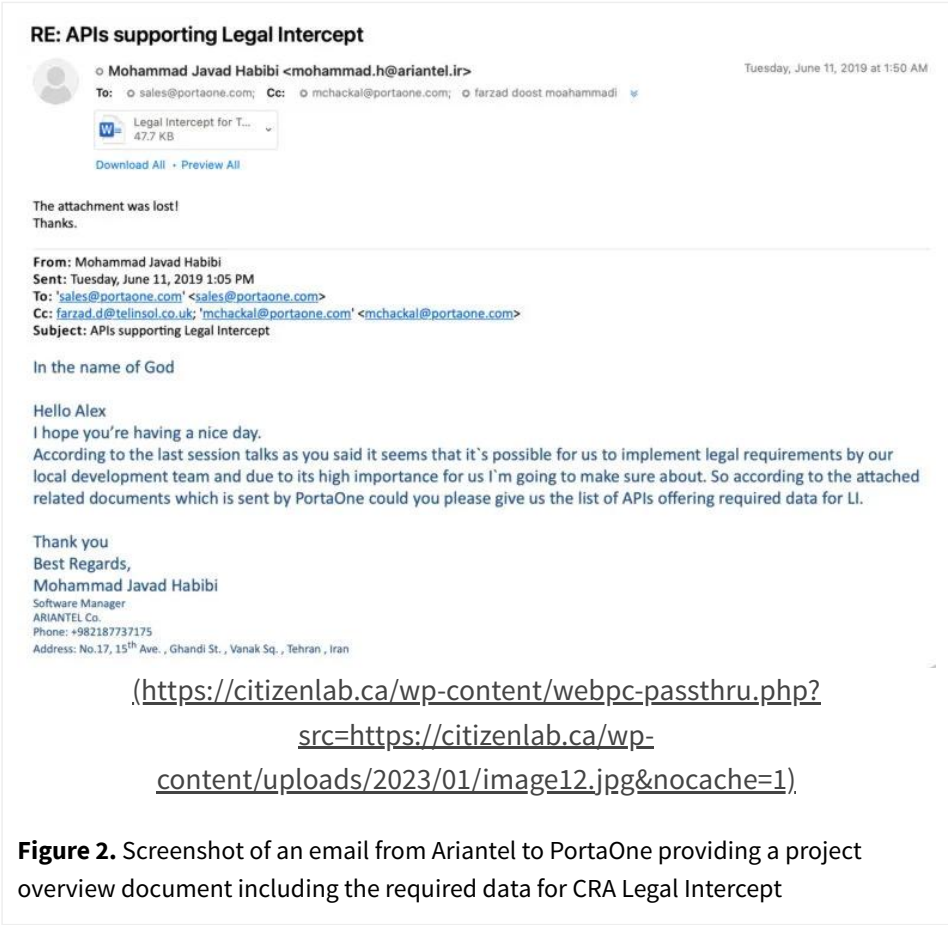
Figure 1. Screenshot of an email from the CRA Directorate General of Communication Security to Ariantel sending the SIAM document

In addition to emails discussing integration requirements and meetings between the vendors regarding Ariantel's MVNO project, the documents we reviewed provide a detailed overview of Iran's system including technical specifications, network diagrams, proposals, and scope of work. An acceptance test document from PROTEI was provided to Ariantel confirming a successful test of "Traffic Management" including Internet service bandwidth restrictions, blocking of certain data services, and logging of Internet usage.

There are multiple mobile network operators within Iran, providing users with many options in their selection of service providers. These options include seven mobile network operators (https://www.gsma.com/coverage/), as well as multiple MVNOs who provide their own branded services using those networks. It is general practice around the world for each mobile service provider to implement systems to provision new users onto their service, bill for the service, offer rate plans, and activate various features. These operations are performed within the service provider's domain of control. However, we discovered that, in Iran, the envisioned domain of control would not belong to the service provider; the domain would be under the administrative control of the CRA legal intercept system (See Figure 2, below). To what extent this vision has been partially or fully implemented since the timeframe of the documents we reviewed is not clear (See Figure 2, below).

The CRA requires that each mobile service provider comply with requirements under a common framework set by the CRA, including directly interfacing with external systems operated by the regulatory authority to ensure legal compliance with information gathering about used services and disabling access to the service.

The Citizen Lab reviewed a document entitled "Legal Intercept", which was authored by an Ariantel employee describing a new MVNO project with Telinsol. The document details the project with solutions to be supplied by PROTEI and PortaOne.



RE: APIs supporting Legal Intercept

Mohammad Javad Habibi <mohammad.h@ariantel.ir> Tuesday, June 11, 2019 at 1:50 AM

To: sales@portaone.com; Cc: mchackal@portaone.com; farzad doost moahammadi

Legal Intercept for T... 47.7 KB

Download All · Preview All

The attachment was lost!
Thanks.

From: Mohammad Javad Habibi
Sent: Tuesday, June 11, 2019 1:05 PM
To: 'sales@portaone.com' <sales@portaone.com>
Cc: farzad.d@telinsol.co.uk; 'mchackal@portaone.com' <mchackal@portaone.com>
Subject: APIs supporting Legal Intercept

In the name of God

Hello Alex
I hope you're having a nice day.
According to the last session talks as you said it seems that it`s possible for us to implement legal requirements by our local development team and due to its high importance for us I`m going to make sure about. So according to the attached related documents which is sent by PortaOne could you please give us the list of APIs offering required data for LI.

Thank you
Best Regards,
Mohammad Javad Habibi
Software Manager
ARIANTEL Co.
Phone: +982187737175
Address: No.17, 15th Ave. , Ghandi St. , Vanak Sq. , Tehran , Iran

(https://citizenlab.ca/wp-content/webpc-passthru.php?src=https://citizenlab.ca/wp-content/uploads/2023/01/image12.jpg&nocache=1)

Figure 2. Screenshot of an email from Ariantel to PortaOne providing a project overview document including the required data for CRA Legal Intercept

This document further describes the Iran Legal Intercept system as based on functional components working in tandem throughout Iran which, as described in documents and communications, include the following:

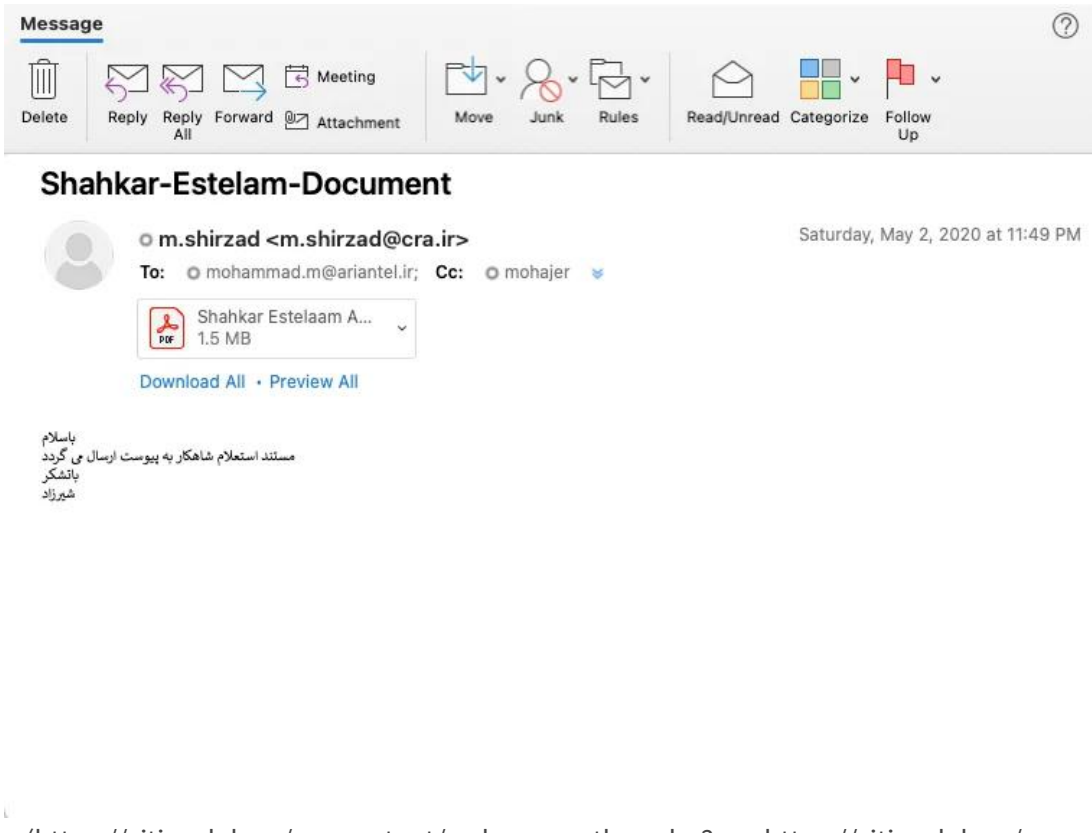
1. **LI (Legal Intercept) System** – The component for conducting usage surveillance and control activity. The LI system gathers information about service usage from individual mobile users and may disable or modify access to the service. The CRA can request detailed usage records to be provided to the LI platform and disable the corresponding services. The LI system uses the SIAM web services API with each mobile service provider in Iran.
2. **CID (Control Illegal Devices) System –** The component for alerting the CRA about changes to a user's service profile of SIM cards provisioned on the network. CID informs the CRA about the current status of active SIM cards currently assigned or which are in the process of being assigned to a user.
3. **SHAHKAR System –** A data warehouse which stores information about all mobile subscribers in Iran to check the "validity of users" and prohibit any registration attempt if the CRA determines the attempt to be invalid. The purpose of the SHAHKAR system is to notify the CRA of users attempting to change to a different service provider, update their subscription information or change their phone number. SHAHKAR prevents users from acquiring new mobile accounts with multiple service providers. Specifically, the documents refer to a use case where a new registration is attempted: "SHAHKAR verifies sent information and sees that this user is signed up with other providers. User creation is prohibited." This description implies that Iran maintains a 1:1 mapping of a user to a SIM profile to simplify its ability to conduct surveillance operations. It provides the CRA with the ability to immediately cancel a user request for a new mobile account or make changes to existing accounts.
4. **SHAMSA –** Shown as an interface for collecting bulk voice and SMS Call Detail Records (CDR's) and data IP Detail Records (IPDR's).

Iran's Legal Intercept Architecture

The Legal Intercept system described in the documents would constitute a significant departure from standardized lawful intercept standards developed by 3GPP (https://www.3gpp.org/technologies/li) working groups and ETSI (https://www.etsi.org/technologies/lawful-interception) standards committees. These standards define processes and interfaces for the exchange of legal warrants, activation of communication interception, and delivering the communication content to the legal authority.

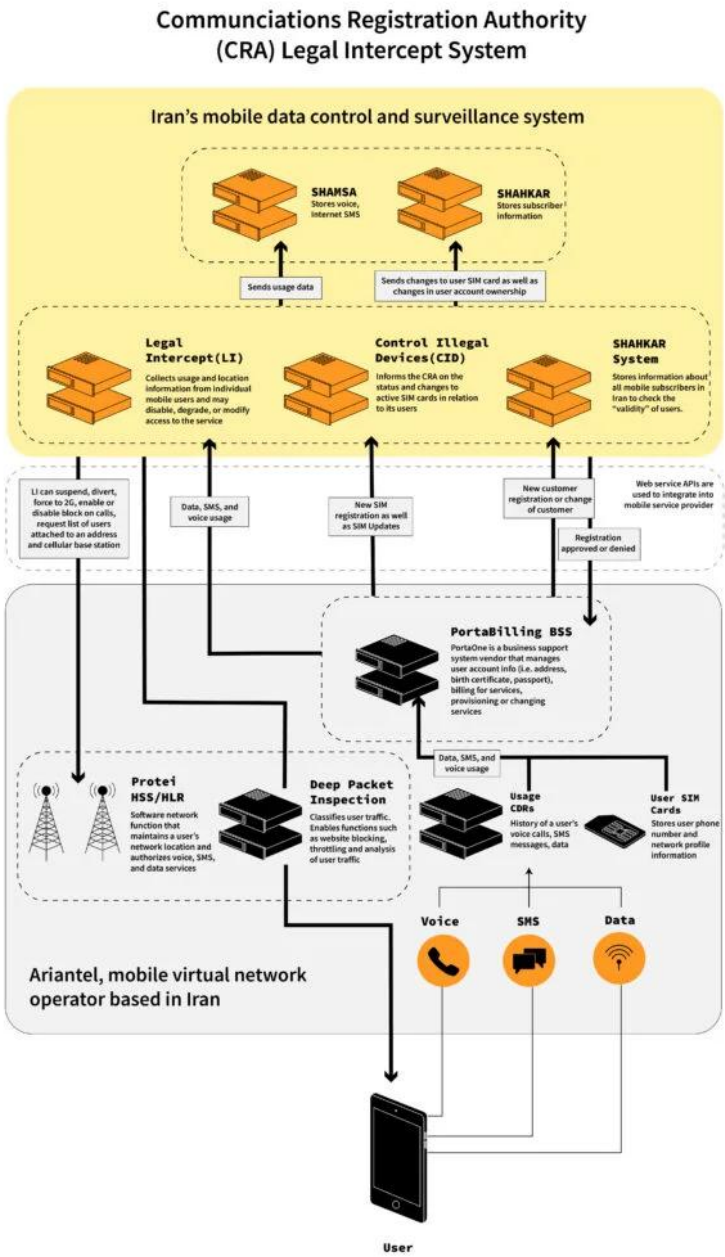
Iran's Legal Intercept system differs from these standards with no facility for legal warrants, blanket delivery of user information during activation, and deep integration into mobile business systems for retrieving user content and changing access to services. Working in concert, the integration of LI, CID, SHAHKAR and SHAMSA components would provide the Iranian government with comprehensive information about Iranian subscribers, including personal information of citizens and non-citizens at the time they purchase SIM cards. The SHAHKAR system, referenced in the email below sent by a CRA staff member to Ariantel, uses a SIM registration API to supply this information during the activation process with mobile service providers, which is then screened by the system to determine whether the SIM activation is approved. Translated to English, the email reads:

```
Hi

The document of Shahkar inquiry is sent as an attachment

Thanks

Shirzad
```



(https://citizenlab.ca/wp-content/webpc-passthru.php?src=https://citizenlab.ca/wp-content/uploads/2023/01/image13.jpg&nocache=1)

Figure 3. Screenshot of an email from a CRA staff member to Ariantel sending the SHAHKAR system document



(https://citizenlab.ca/wp-content/webpc-passthru.php?src=https://citizenlab.ca/wp-content/uploads/2023/01/legal-intercept-111323-scaled.jpg&nocache=1)

Figure 4. Diagram prepared by the Citizen Lab which shows the relationship between Iran's Legal Intercept System Interfaces and Mobile Service Provider Systems along with examples of Legal Intercept System Commands that query user information and control services

The diagram above, created by the Citizen Lab from technical specifications in the documents, shows elements selected by Ariantel which would play key roles in Iran's legal intercept capabilities. These elements include the business support system providing usage CDR's, SIM card updates, and the HLR/HSS (Home Location Register and Subscriber Server), which maintains a user's network location and authorizes voice, SMS, and data services. The LI component uses multiple API commands to query user information and issue control commands to the mobile service provider in real time. It also defines a process to pull historical usage details, such as CDR's, from the mobile service provider systems into SHAMSA for storage.

The documents show that products from Canadian-based vendor PortaOne and PROTEI, including the *PortaBilling* Converged Business Support System (BSS), were selected by Ariantel to provide information to Iran's Legal Intercept system components. While we have no evidence that final agreements were executed for this system, the discussions around its implementation appear to have been well-advanced. The BSS is the primary mobile system used for storing information about customers, configuring and billing for services, and managing services such as provisioning new or changing existing user services. The PortaOne system integrates with systems provided by PROTEI, and, if implemented, would supply detailed usage information to the Legal Intercept system while receiving information about requests for new or updated services (all without user knowledge). In addition, commands from the CRA interact with the Ariantel network to suspend and control voice and data services and supply the location of users on the network.

The surveillance and censorship capabilities resulting from this level of integration with mobile service providers cannot be understated. Because Iranian authorities would receive information from all mobile service providers, they would have deep visibility into all services used, who is communicating with whom, for how long, how often, and where. They could also identify the current phone numbers used in certain geographic areas based on CellID or street address. This information could be used to decide who, what, and when to place restrictions or make changes to a user's mobile service plan, such as the user's social community or the location of political demonstrations. They could also view extensive personally identifiable details when users sign up for mobile services including:

1. Name
2. Family
3. Father's name
4. Number of birth certificate
5. Birth date
6. Birthplace
7. Home Telephone Number
8. Email Address
9. Gender
10. Zip Code
11. Nationality
12. Passport Number
13. Postal Address/Home Addresses

Findings: Iranian Mobile Surveillance and Control Real Time API

The documents show API commands used by Iranian authorities to query user information and change user services. Citizen Lab researchers have extracted the API commands from the SIAM document and grouped them into the tables (presented below) to show those that could be used for surveillance, for modifying services, and testing results for enforcing bandwidth restrictions of data applications.

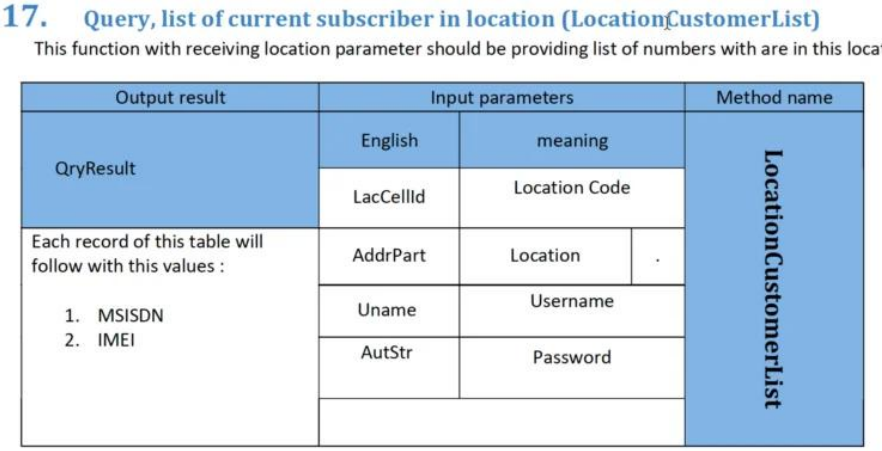
SURVEILLANCE-RELATED API COMMANDS (SIAM Web Service)

The following commands allow the CRA to search for users and retrieve personal information and related usage.

The commands span virtually all usage associated with a mobile user, or a collection of users within a specific location. The CRA can use the SIAM API with a user parameter (Name, Family, Passport, IP Address, Phone Number, MAC Address, IMEI, etc.) to request information. The API documentation also indicates that Iran may have visibility into the type of network available to the user termed as "Connection base" (such as cellular versus WiFi).

API REQUEST	DESCRIPTION
GetIPDR	Request information on a user's Internet sessions tdat took place during a specific time period.
GetCdr	Request information on the history of a user's voice calls and SMS messages.
FullSearchByNum	Request details about a user's mobile service and personal details.
BillingInfoSearch	Request details about a user's mobile service financial transactions.
ListOfPhoneServices	Request details about the different mobile services available to a user.
DivertInfoSearch	Request details about a user's call forwarding status.
LocationCustomerList	Request a list of phone numbers in a geo-location by providing the LaCellId (Location Area Code+Cell ID) ar
ApnOwnerSearch	Request the owner of a particular APN (Access Point Name).

Table 1. Table compiled by the Citizen Lab showing a list of required SIAM API surveillance query methods used by Iran CRA



17. Query, list of current subscriber in location (LocationCustomerList)

This function with receiving location parameter should be providing list of numbers with are in this location

Output result	Input parameters		Method name
QryResult	English	meaning	LocationCustomerList
	LacCellId	Location Code	
Each record of this table will follow with this values : 1. MSISDN 2. IMEI	AddrPart	Location .	
	Uname	Username	
	AutStr	Password	

(https://citizenlab.ca/wp-content/webpc-passthru.php?src=https://citizenlab.ca/wp-content/uploads/2023/01/image17.png&nocache=1)

Figure 5. Screenshot from SIAM documents showing the command used to retrieve mobile phone users at a geographic location

CONTROL-RELATED API COMMANDS (SIAM Web Service)

The following commands (Table 2) allows the CRA to apply immediate changes to a user's service and remove the requested changes when no longer required.

Media stories suggest that Iran has employed controls to shut down mobile services or block Internet traffic (https://www.theguardian.com/world/2022/sep/22/iran-blocks-capitals-internet-access-as-amini-protests-grow). We can confirm through the documentation shared with the Citizen Lab that in addition to blocking services, the CRA could change call forwarding rules, force the phone to use a slower 2G network, and block access to services

based on location. This API allows Iranian authorities to have the flexibility to place partial blocks on phone calls or data services, allowing authorities to apply network policies in a highly granular manner, such as blocking incoming or outgoing calls or modify certain call forwarding criteria.

API REQUEST	DESCRIPTION
ApplySusp	
ApplySuspIP	Block incoming, outgoing, all voice calls or disconnect a call currently in progress. Block all current data sessions
ApplyDivert	Remove a user's call forwarding settings or forward all incoming calls to another number.
Force2GNumber	Disable all 3G and 4G data services, forcing a user's phone to only use 2G data speeds.
SuspOrder	Block an order for a mobile service or prevent a user's request to change a mobile service.

Table 2. Citizen Lab created list of required SIAM API blocking commands used by Iran CRA

The screenshot below taken from the SIAM document shows the command used for blocking data services:

6. Request for Disable and Enable connection\ service (ApplySuspIp)

This function will be used to disconnect or connect a data connection or service. If the operator receives one or a combination of the parameters in the input, the request type (disconnect / connect) and the determination of other parameters, the request (disconnect / connect or service) must be returned by returning the response in a row to the Siam

Allowed Value for SuspType can be finding in below table:

Operation	Value
Temporary termination of subscriber to release dynamic IP from line	0
Permanent Suspension/termination	1
suspension for 24 hour	2
suspension for 3 day	3
suspension for 1 week	4
suspension for 15 day	5

(https://citizenlab.ca/wp-content/webpc-passthru.php?src=https://citizenlab.ca/wp-content/uploads/2023/01/image7-1.jpg&nocache=1)

Figure 6. Screenshot from SIAM documents showing the command used for blocking data services for a time period

IP TRAFFIC MANAGEMENT

While not listed explicitly in the SIAM API document, the Citizen Lab reviewed an acceptance test document from PROTEI, performed on behalf of Ariantel, verifying that data services can be restricted based on multiple criteria – as shown in the screenshot below from the document. The PROTEI DPI can classify user data into service types, such as WhatsApp, Facebook, or Twitter and restrict the bandwidth/Quality of Service (QoS) of that service type, making the service unusable. It allows for the following commands:

1. Restrict bandwidth for certain websites or apps for a user

2. Block data traffic for certain websites or apps for a user
3. Block all data for a user
4. Block all data for all users

1.1.5. Traffic Management

Test name	**1.1.19 Traffic bandwidth restrictions by certain services**
Goal	To verify traffic bandwidth restrictions by certain services
Initial conditions	Service which bandwidth must be limited is configured in DPI, subscriber profile is created on PCRF and has linked bundle with specified QoS for DPI service.
Scenario	1. Subscriber activates session; 2. PGW sends Access-Request with User-Name to DPI; 3. DPI sends CCR-I with User-Name to PCRF; 4. PCRF sends CCA-I with permitting PCC-rules with limited QoS to DPI; 5. DPI sends Access-Accept to PGW; 6. PGW sends Accounting-Request Start with delegated IP-address to DPI; 7. DPI sends CCR-U with delegated IP-address to PCRF; 8. PCRF sends CCA-U to DPI; 9. DPI sends Accounting-Response to PGW; 10. Check subscriber access and enforced QoS limitation for DPI service.
Result	Success Date: 2020-10-27 Time: 16:00: [redacted] number : 989998800891
Comments	

(https://citizenlab.ca/wp-content/webpc-passthru.php?src=https://citizenlab.ca/wp-content/uploads/2023/01/image9.jpg&nocache=1)

Figure 7. Screenshot from the PROTEI DPI Acceptance Test Protocol document showing a successful test of bandwidth restriction performed for the Iran MVNO Ariantel

These commands and test cases (shown in Figure 16) from PROTEI show the extensive data restriction capabilities available to the CRA via deep mobile network integration to mitigate user communications inside and outside of Iran.

Foreign Corporate Entities: Telinsol, PROTEI, and PortaOne

Our review of the documents provided by *The Intercept* suggests that companies based in the UK, Russia, and Canada explored providing commercial services that, based on our review of the documents, would support the CRA's surveillance, control, and account management capabilities.

Prior to publishing this report, on January 4, 2023, we provided a summary of our research findings to Telinsol (https://citizenlab.ca/wp-content/uploads/2023/01/Telinsol_January-4-2023.pdf), PROTEI (https://citizenlab.ca/wp-content/uploads/2023/01/PROTEI_January-4-2023.pdf), and PortaOne (https://citizenlab.ca/wp-content/uploads/2023/01/PortaOne_January-4-2023.pdf) and offered them a week to respond along with an undertaking to publish their response in full. We received a response from PortaOne (https://citizenlab.ca/wp-content/uploads/2023/01/PortaOnetoCL_January112023.pdf) on January 11, 2023 and the company made an official statement (https://citizenlab.ca/wp-content/uploads/2023/01/PortaOne_OfficialStatement_January-112023.pdf) on January 11, 2023. We received a response from Telinsol (https://citizenlab.ca/wp-content/uploads/2023/01/TelinsoltoCL_January-112023.pdf) on January 11, 2023, and another on January 13, 2023. All responses and the official statement have been included as Appendix C to the report.

Telinsol Ltd.

Telinsol Ltd. (https://www.telinsol.com/) is a UK-based telecommunications company that was founded in 2015 (https://find-and-update.company-information.service.gov.uk/company/09576707). It is a private limited company (https://find-and-update.company-information.service.gov.uk/company/09576707) that, according to their website

(https://www.telinsol.com/), engages in telecommunications and information technology consulting, support services, equipment supply, and satellite telecommunications. We viewed the company's LinkedIn page on December 6, 2022, but it has since been removed.

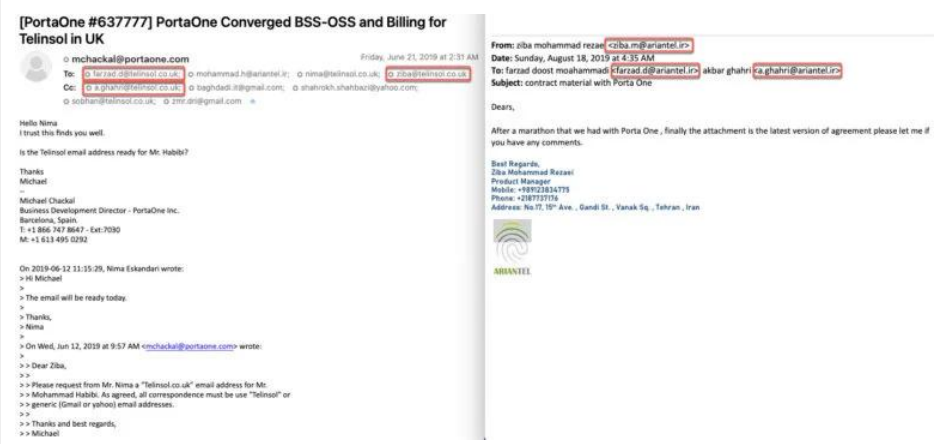
Nima Eskandari, an Iranian national (https://find-and-update.company-information.service.gov.uk/company/09576707/officers), is one of the company's two listed directors (https://find-and-update.company-information.service.gov.uk/company/09576707/officers) (the other director is identified as Simon Edward Maddox). Mr. Eskandari describes himself as the company's founder on LinkedIn and is identified as the company's Managing Director in email correspondence. Mr. Maddox was listed as an employee of Telinsol on the company's LinkedIn profile before it was taken down. He has kept a reference to the company in his LinkedIn byline.

We also noted that, on December 6, 2022 when we viewed his LinkedIn profile, an individual called Akbar Ghahri identified himself as "Head of Satellite Services" at Telinsol from January 2021-Present, while also identifying himself as "Managing Director" of SamanTel, which describes itself as the first MVNO license holder in Iran (https://www.linkedin.com/company/samantel/) from October 2020-Present. Mr. Ghahri appears to have removed the reference to Telinsol on his LinkedIn profile. In what appears to be his Twitter profile, Mr. Ghahri identifies himself as working for a telecommunications company and being based in Iran, while his LinkedIn profile lists that he is based in the UK. On this webpage (https://data-lead.com/person/name/Akbar+Gh/id/727347495/v/cad86), an "Akbar Gh" is identified as a satellite engineer at Telinsol.

There are several other ties between Telinsol and Iran, including evidence suggesting that Telinsol, as a UK-based company, may be working on behalf of Ariantel (https://ariantel.ir/).

In one document we reviewed, which was sent by an Ariantel software manager as an attachment to individuals at PortaOne, Ariantel, and Telinsol, the following language is included: "Telinsol is [sic] Mobile Virtual Network Operator in Iran"[1] and that "[t]o provide services in Iran every MVNO must comply with legal requirements and have Legal Intercept." The document goes on to describe the Legal Intercept system in Iran.

Documents attached in the emails shared with the Citizen Lab appear to show Telinsol facilitating purchases to support Ariantel's MVNO launch, including SIM cards, the PortaOne solution, and coordinating meeting logistics for training Ariantel staff on the operation of the PROTEI DPI solution. Direct email communications between Mr. Eskandari, PortaOne, and Ariantel include commercial proposals, equipment purchase orders, training, logistics, and contract details. As evidenced by the screenshots of emails below from June and August 2019, an agreement appears to have been concluded among the parties that Ariantel representatives use Telinsol, Gmail or Yahoo email addresses to communicate. A comparison of the two emails confirms that Ariantel representatives are using both Telinsol and Ariantel email addresses, suggesting an affiliation between the companies.

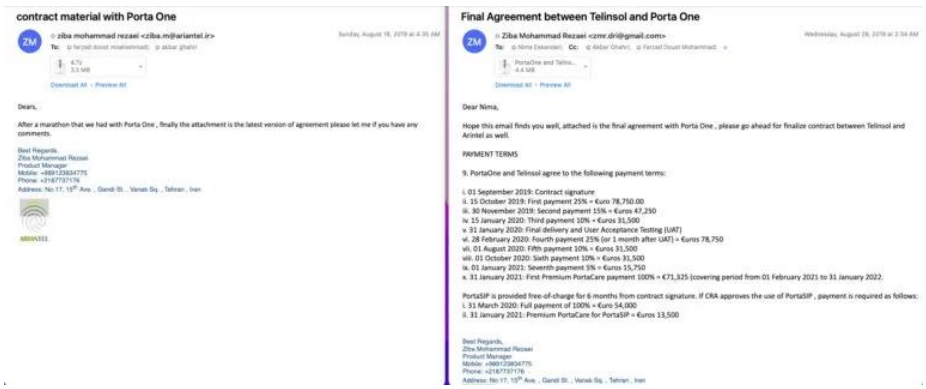


(https://citizenlab.ca/wp-content/webpc-passthru.php?

src=https://citizenlab.ca/wp-content/uploads/2023/01/image6.jpg&nocache=1)

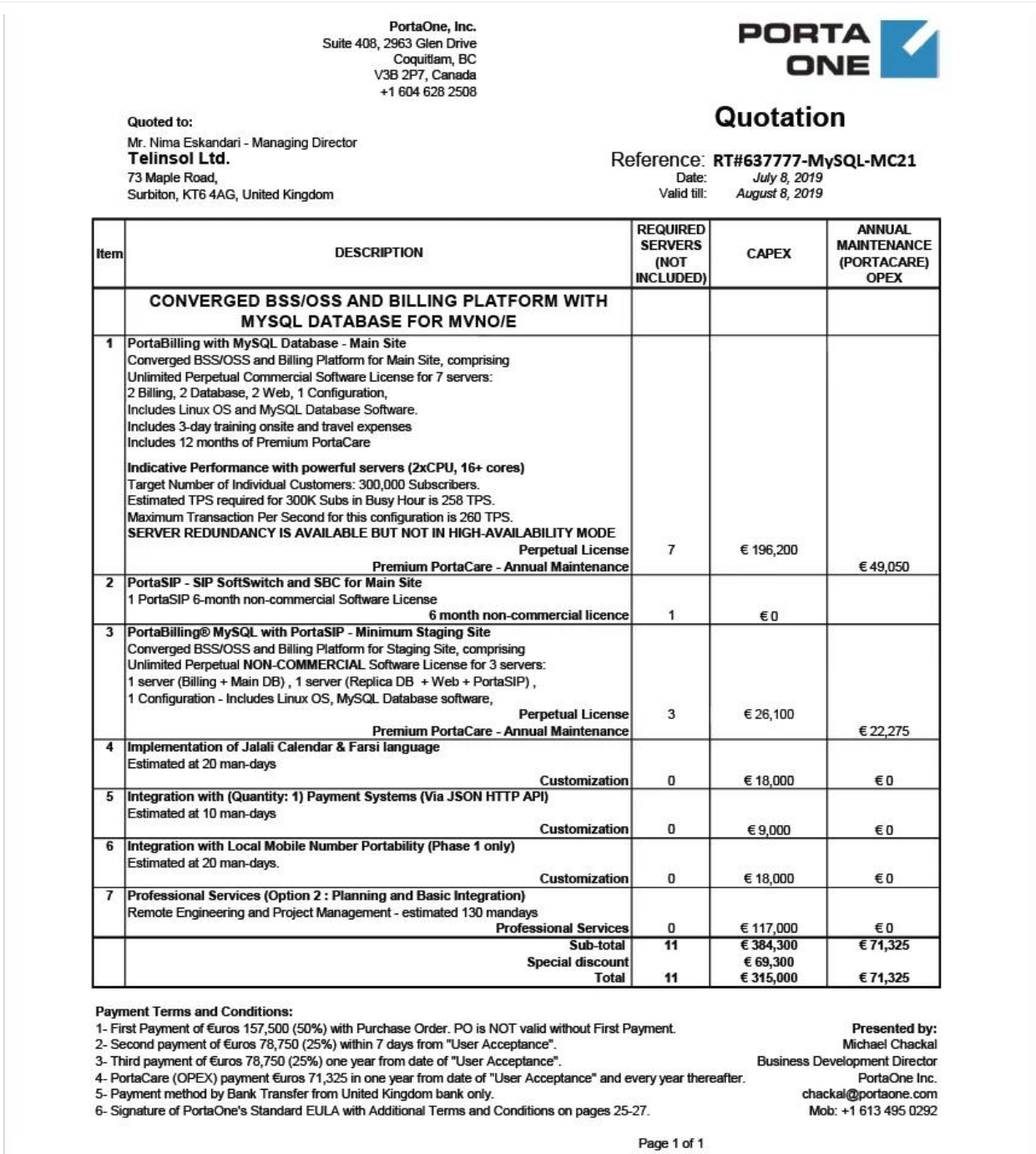
Figure 8. Screenshot of an email requesting the use of Telinsol Gmail or Yahoo email addresses to communicate and an email of the same users with both Telinsol and Ariantel email addresses

Internal Ariantel emails shown below reference commercial material provided in .zip files, including commercial documents from PortaOne to Mr. Eskandari.



(https://citizenlab.ca/wp-content/webpc-passthru.php?src=https://citizenlab.ca/wp-content/uploads/2023/01/image7.jpg&nocache=1)

Figure 9. Screenshots of internal Ariantel emails referencing commercial agreement documents with PortaOne



PortaOne, Inc.
Suite 408, 2963 Glen Drive
Coquitlam, BC
V3B 2P7, Canada
+1 604 628 2508

PORTA ONE

Quotation

Quoted to:
Mr. Nima Eskandari - Managing Director
Telinsol Ltd.
73 Maple Road,
Surbiton, KT6 4AG, United Kingdom

Reference: **RT#637777-MySQL-MC21**
Date: *July 8, 2019*
Valid till: *August 8, 2019*

Item	DESCRIPTION	REQUIRED SERVERS (NOT INCLUDED)	CAPEX	ANNUAL MAINTENANCE (PORTACARE) OPEX
	CONVERGED BSS/OSS AND BILLING PLATFORM WITH MYSQL DATABASE FOR MVNO/E			
1	**PortaBilling with MySQL Database - Main Site** Converged BSS/OSS and Billing Platform for Main Site, comprising Unlimited Perpetual Commercial Software License for 7 servers: 2 Billing, 2 Database, 2 Web, 1 Configuration, Includes Linux OS and MySQL Database Software. Includes 3-day training onsite and travel expenses Includes 12 months of Premium PortaCare **Indicative Performance with powerful servers (2xCPU, 16+ cores)** Target Number of Individual Customers: 300,000 Subscribers. Estimated TPS required for 300K Subs in Busy Hour is 258 TPS. Maximum Transaction Per Second for this configuration is 260 TPS. **SERVER REDUNDANCY IS AVAILABLE BUT NOT IN HIGH-AVAILABILITY MODE** **Perpetual License** **Premium PortaCare - Annual Maintenance**	7	€ 196,200	€ 49,050
2	**PortaSIP - SIP SoftSwitch and SBC for Main Site** 1 PortaSIP 6-month non-commercial Software License **6 month non-commercial licence**	1	€ 0	
3	**PortaBilling® MySQL with PortaSIP - Minimum Staging Site** Converged BSS/OSS and Billing Platform for Staging Site, comprising Unlimited Perpetual **NON-COMMERCIAL** Software License for 3 servers: 1 server (Billing + Main DB) , 1 server (Replica DB + Web + PortaSIP) , 1 Configuration - Includes Linux OS, MySQL Database software, **Perpetual License** **Premium PortaCare - Annual Maintenance**	3	€ 26,100	€ 22,275
4	**Implementation of Jalali Calendar & Farsi language** Estimated at 20 man-days **Customization**	0	€ 18,000	€ 0
5	**Integration with (Quantity: 1) Payment Systems (Via JSON HTTP API)** Estimated at 10 man-days **Customization**	0	€ 9,000	€ 0
6	**Integration with Local Mobile Number Portability (Phase 1 only)** Estimated at 20 man-days. **Customization**	0	€ 18,000	€ 0
7	**Professional Services (Option 2 : Planning and Basic Integration)** Remote Engineering and Project Management - estimated 130 mandays **Professional Services**	0	€ 117,000	€ 0
	Sub-total **Special discount** **Total**	**11** **11**	**€ 384,300** **€ 69,300** **€ 315,000**	**€ 71,325** **€ 71,325**

Payment Terms and Conditions:
1- First Payment of €uros 157,500 (50%) with Purchase Order. PO is NOT valid without First Payment.
2- Second payment of €uros 78,750 (25%) within 7 days from "User Acceptance".
3- Third payment of €uros 78,750 (25%) one year from date of "User Acceptance".
4- PortaCare (OPEX) payment €uros 71,325 in one year from date of "User Acceptance" and every year thereafter.
5- Payment method by Bank Transfer from United Kingdom bank only.
6- Signature of PortaOne's Standard EULA with Additional Terms and Conditions on pages 25-27.

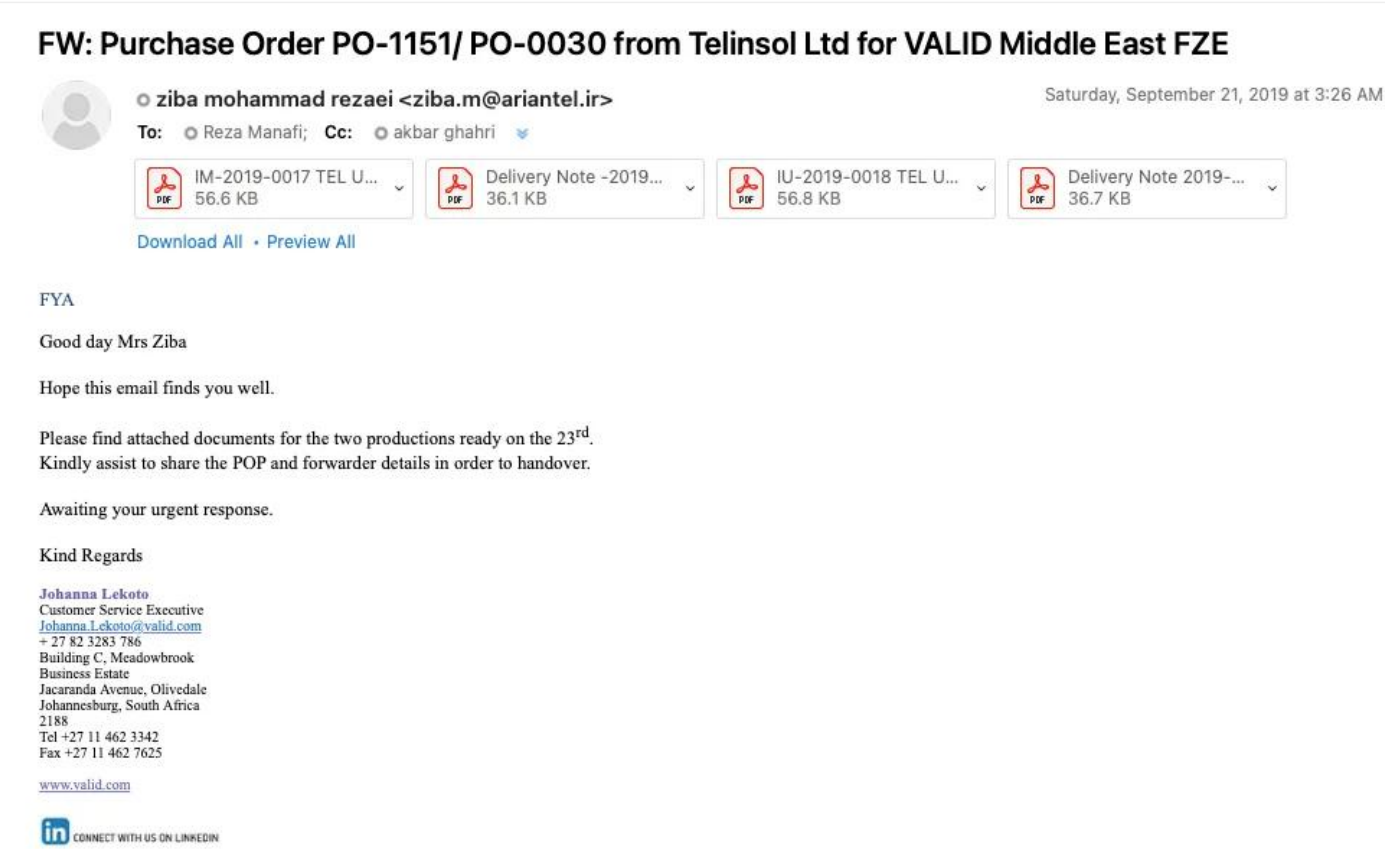
Presented by:
Michael Chackal
Business Development Director
PortaOne Inc.
chackal@portaone.com
Mob: +1 613 495 0292

Page 1 of 1

(https://citizenlab.ca/wp-content/webpc-passthru.php?src=https://citizenlab.ca/wp-content/uploads/2023/01/image3.jpg&nocache=1)

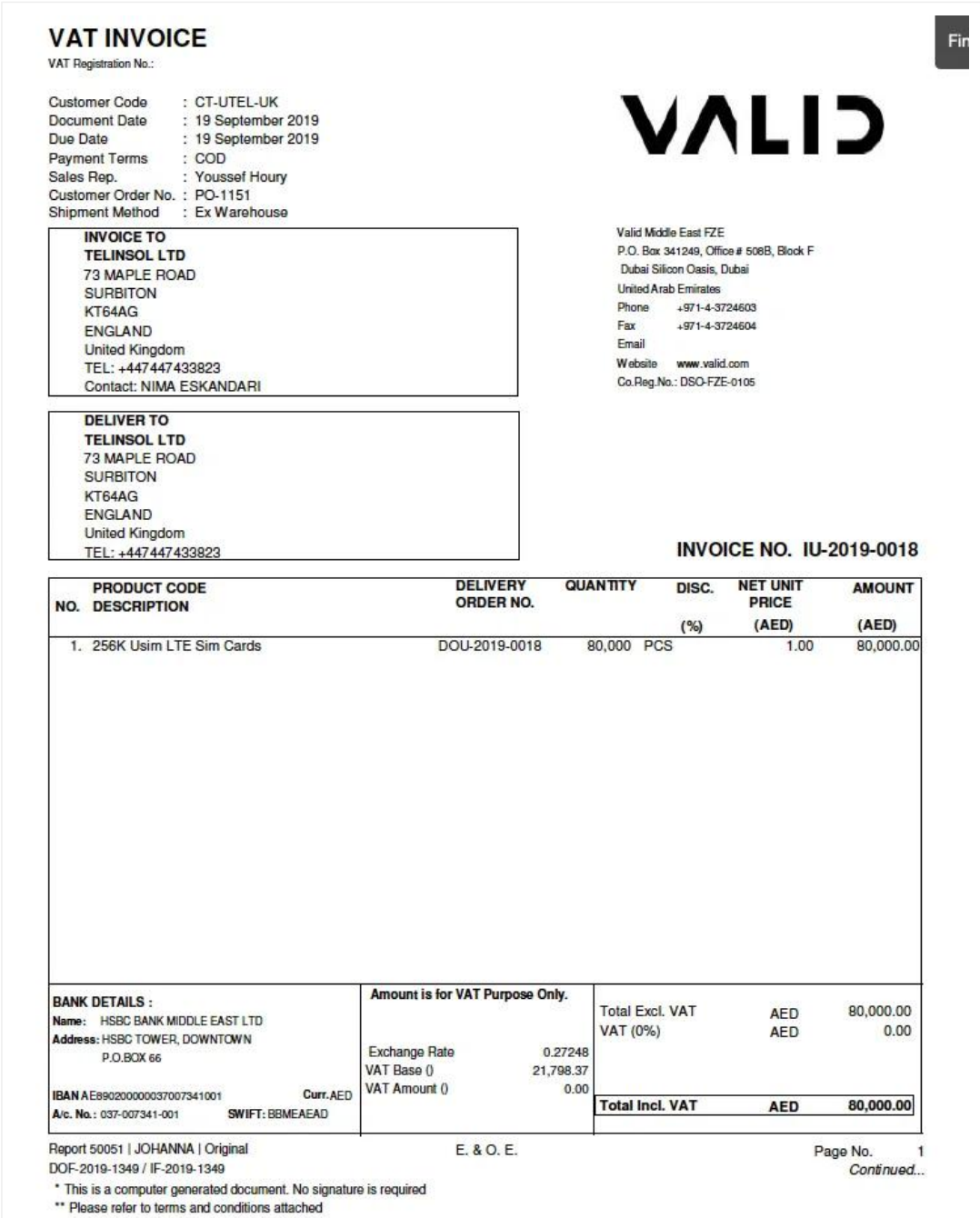
Figure 10. Screenshot of a PortaOne commercial quotation to Telinsol

In addition to the PortaOne quotation, an invoice was sent from Valid, a Brazil-based SIM Card provider, to Ariantel email recipients referencing a Telinsol purchase order, further suggesting that Telinsol may have acted as a procurement partner with Ariantel.



(https://citizenlab.ca/wp-content/webpc-passthru.php?src=https://citizenlab.ca/wp-content/uploads/2023/01/image2.jpg&nocache=1)

Figure 11. Screenshot of an email sent to Ariantel including attached invoices issued to Telinsol for SIM card purchases



VAT INVOICE

VAT Registration No.:

Customer Code : CT-UTEL-UK
Document Date : 19 September 2019
Due Date : 19 September 2019
Payment Terms : COD
Sales Rep. : Youssef Houry
Customer Order No. : PO-1151
Shipment Method : Ex Warehouse

VALID

INVOICE TO
TELINSOL LTD
73 MAPLE ROAD
SURBITON
KT64AG
ENGLAND
United Kingdom
TEL: +447447433823
Contact: NIMA ESKANDARI

Valid Middle East FZE
P.O. Box 341249, Office # 508B, Block F
Dubai Silicon Oasis, Dubai
United Arab Emirates
Phone +971-4-3724603
Fax +971-4-3724604
Email
Website www.valid.com
Co.Reg.No.: DSO-FZE-0105

DELIVER TO
TELINSOL LTD
73 MAPLE ROAD
SURBITON
KT64AG
ENGLAND
United Kingdom
TEL: +447447433823

INVOICE NO. IU-2019-0018

NO.	PRODUCT CODE DESCRIPTION	DELIVERY ORDER NO.	QUANTITY	DISC. (%)	NET UNIT PRICE (AED)	AMOUNT (AED)
1.	256K Usim LTE Sim Cards	DOU-2019-0018	80,000 PCS		1.00	80,000.00

BANK DETAILS :
Name: HSBC BANK MIDDLE EAST LTD
Address: HSBC TOWER, DOWNTOWN
P.O.BOX 66
IBAN AE890200000037007341001 Curr.AED
A/c. No.: 037-007341-001 SWIFT: BBMEAEAD

Amount is for VAT Purpose Only.
Exchange Rate 0.27248
VAT Base () 21,798.37
VAT Amount () 0.00

Total Excl. VAT	AED	80,000.00
VAT (0%)	AED	0.00
Total Incl. VAT	**AED**	**80,000.00**

Report 50051 | JOHANNA | Original
DOF-2019-1349 / IF-2019-1349
E. & O. E.
Page No. 1
Continued...
* This is a computer generated document. No signature is required
** Please refer to terms and conditions attached

(https://citizenlab.ca/wp-content/webpc-passthru.php?src=https://citizenlab.ca/wp-content/uploads/2023/01/image11.jpg&nocache=1)

Figure 12. Screenshot of an invoice for SIM Cards ordered by Telinsol and included in the email attachment sent to Ariantel

Mr. Eskandari was also seen facilitating meetings between Iranian-based Ariantel and Russian-based PROTEI personnel as evidenced by the emails below.

Mr. Eskandari and fellow Telinsol Director, Mr. Maddox, are also directors (https://find-and-update.company-information.service.gov.uk/company/11651795/officers) of Emeatra Ltd (https://emeatra.com/)., another UK-based company that supplies new and used telecommunications and network equipment. They are also directors (https://find-and-update.company-information.service.gov.uk/company/13735444) in another UK-based company called Agtelligence Ltd. (https://www.agtelligence.space/), which is described on LinkedIn (https://www.linkedin.com/company/agtelligence/about/) as "[h]elping UK farmers on their journey to sustainability."

Response from Telinsol

On January 11, 2023, DLA Piper (Canada) LLP sent an email to the Citizen Lab on behalf of Telinsol. In this response, Telinsol stated that it:

> …flatly denies the allegation that it has been involved in activities that would in any way help digital espionage against Iranian citizens. In particular, the suggestion in your letter that Telinsol provides commercial services to support Iran's Legal Intercept requirements of mobile surveillance, service control and account management is entirely false and any publication of such an allegation would cause irreparable harm to Telinsol, as well as to the reputation of its past and present clients.

The company further urged the Citizen Lab to "eliminate any reference to Telinsol in its report" and that it would "not hesitate to avail itself of all available legal remedies in response to a defamatory publication by Citizen Lab."

In a subsequent letter dated January 13, 2023, DLA Piper (Canada) LLP followed up with another letter on behalf of Telinsol. In this letter, Telinsol stated, via counsel, that the "hacked emails evidence a relationship between Ariantel and PortaOne which pre-dates the involvement of Telinsol." The emails "further evidence Telinsol entertaining an initial enquiry by Ariantel and PortaOne and thereafter entering a due diligence process – a due diligence process that ended in September, 2019 with Telinsol rejecting involvement in the project." Telinsol also claims that "any activities that thereafter continued were with a Portugal-based company called Magicalcharacter."

As noted in this report, the documents we reviewed did not include a signed agreement between Telinsol and Ariantel. However, the correspondence reviewed above, which took place in 2019, did include a number of indications that Telinsol may have been acting as a procurement partner with Ariantel at one point in time, as well as email exchanges involving Telinsol, PortaOne, PROTEI, and Ariantel.

Further, we also reviewed one email chain from 2021 between Telinsol, PROTEI, and Ariantel. In this correspondence the NFV EPC & PS Core Manager at Ariantel writes to Mr. Eskandari (Telinsol's Director): "[k]indly based on our phone conversation and CEO order, please arrange PROTEI training team to come to Iran." In this same email chain, Mr. Eskandari (Telinsol's Director) asks "Vladimir," an individual who appears to be working at PROTEI Russia, what the current travel policy is in Russia and whether it would be "possible to fly to Iran."

This email chain was dated 2021, suggesting that Telinsol had some kind of involvement with Ariantel that arose after September 2019. It is not clear based on the documents we reviewed whether this correspondence from 2021 relates to the earlier discussions between PortaOne, Telinsol, and Ariantel that arose in 2019.

From: Nima Eskandari <nima@telinsol.co.uk>
Date: Monday, July 12, 2021 at 11:30 PM
To: Фрейнкман Володя <vf@protei.ru>
Cc: rasool alipour <r.alipour@ariantel.ir>, Moein Mirmoeini <Moein.m@ariantel.ir>, kamran baratnejad <kamran.b@ariantel.ir>, Artur Mikhailov <mikhailov@protei.ru>
Subject: Re: Protei Training

Dear Vladimir

What's the current travel policy in Russia? Would it be possible to fly to Iran?

I am looking forward to hearing from you.

Best Regards,

Nima Eskandari MBCS - Managing Director
TELINSOL LTD
73 Maple Road
Surbiton
KT6 4AG
United Kingdom
Mobile: +44 7447433823
Office: +44 2032909656

The information in this email is confidential and solely for the use of the intended recipient(s). If you receive this email in error, please notify the sender and delete the email from your system immediately. In such circumstances, you must not make any use of the email or its contents.
Views expressed by an individual in this email do not necessarily reflect the views of Telinsol Ltd.

Telinsol Ltd.
Registered office: 73 Maple Road, Surbiton, United Kingdom, KT6 4AG. Registered in England.
Registered number: 09576707.

On 13 Jul 2021, at 05:19, Moein Mirmoeini <Moein.m@ariantel.ir> wrote:

Dear Nima,

Hope you are doing well.

Kindly based on our phone conversation and CEO order, please arrange PROTEI training team to come to Iran.

Thanks.

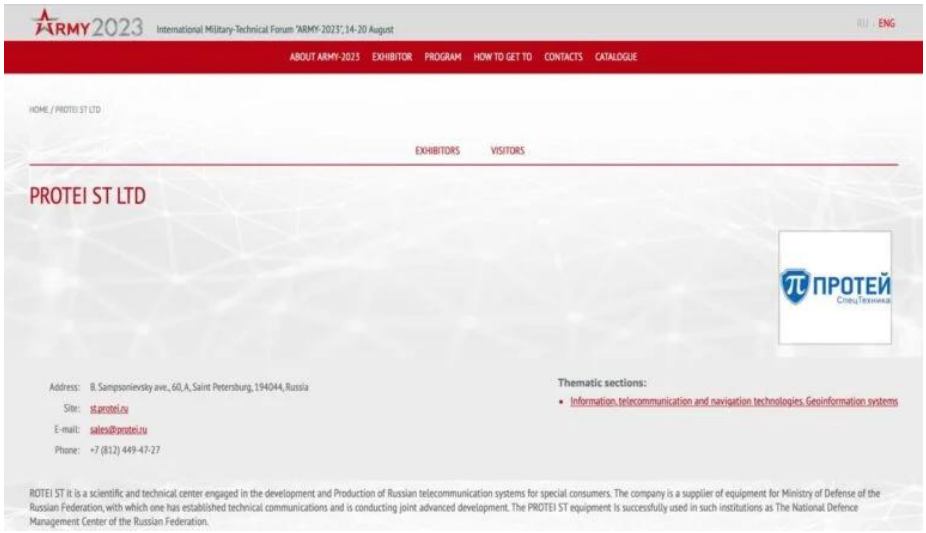
<image001.png>
Best Regards,
Moein Mirmoeini
NFV EPC & PS Core Manager
Mobile: +98-9998800831
No.17, 15th Ave. , Ghandi St. , Vanak Sq. , Tehran , Iran

(https://citizenlab.ca/wp-content/webpc-passthru.php?src=https://citizenlab.ca/wp-content/uploads/2023/01/image1.jpg&nocache=1)

Figure 13. Screenshot of an email dialogue between Nima Eskandari, Ariantel and PROTEI regarding training venue logistics between Russia and Iran

PROTEI Ltd.

PROTEI Ltd. (https://protei.com/) is a Russian telecommunications, software and hardware company founded in 2002 and operating (https://protei.com/company) in Eastern Europe, Asia, Latin America, North Africa and the Middle East. While PROTEI advertises its headquarters in Estonia (https://ariregister.rik.ee/eng/company/14162440/PROTEI-EUROPA-O%C3%9C?search_id=78b9859&pos=10) and its Middle East and Northern Africa (MENA) branch in Jordan (https://www.info-clipper.com/en/company/jordan/protei-mena.jod980qqt.html?retry=1), its Russian origins are not widely advertised. The original PROTEI, called "PROTEI NTC" (Scientific-Technological Center PROTEI), is located in Saint-Petersburg. PROTEI has a dedicated Russian branch, PROTEI ST (http://www.st.protei.ru/) or "Special Technical Centre," created (https://protei-st.ru/) to work with government agencies and military departments in the Russian Federation, including the Ministry of Defence and the National Defence Management Centre (https://rusarmyexpo.com/4326/en/catalog_exhibitors/members/43836).



(https://citizenlab.ca/wp-content/webpc-passthru.php?src=https://citizenlab.ca/wp-content/uploads/2023/01/image8.jpg&nocache=1)

Figure 14. PROTEI Exhibitor Page "Army-2023" Military Technical Forum at Kubinka Air Base, Moscow

PROTEI is involved in developing a wide range (https://protei-st.ru/products/mks/) of solutions for special communications (videoconferencing, Internet and mobile connectivity for the Russian army), but also DPI solutions. These technologies were exported to Kyrgyzstan (https://www.protei.me/new-installation-of-protei-dpi-platform/), Uzbekistan (https://protei.ru/news/edinyy-cov-protey-dlya-ak-uzbektelekom),[2] Tajikistan (https://www.protei.me/protei-built-mvno-core-for-mtt/), Niger (https://www.protei.me/protei-launches-a-new-dpi-platform-in-niger/), and Bahrain (https://www.protei.me/nuetel-launches-protei-dpi-platform/). PROTEI representatives also visited (https://sana.sy/en/?p=274898) Syria in August 2022 to discuss potential collaboration.

PROTEI has partnered with PortaOne, integrating numerous products between the two companies. In a joint press release in 2017 the companies announced the integration of PortaOne's PortaBilling Business Support System (BSS) and PROTEI's Home Location Register HLR/HSS (https://markets.businessinsider.com/news/stocks/portaone-and-protei-expand-joint-intelligent-network-offering-to-include-hlr-hss-and-pcrf-support-1008287844) and Policy Controller PCRF products, which enables MVNOs to manage subscribers and services independently of host network operators, and to launch new mobile networks. They had previously integrated PortaBilling BSS with PROTEI's CAMEL Gateway and DPI Platform in 2016 (https://markets.businessinsider.com/news/stocks/portaone-and-protei-expand-joint-intelligent-network-offering-to-include-hlr-hss-and-pcrf-support-1008287844), which functions as a mechanism to enforce broadband usage policies. According to PortaOne documents (https://drive.google.com/file/d/1pYgoxek_0BWfYplCVftM_ywScP3doQZt/view?usp=share_link), there is also interoperability with PROTEI PCRF, PROTEI PGW, PROTEI SMSC, and PROTEI USSD Gateway. In 2020, PROTEI and PortaOne announced (https://www.protei.me/protei-and-portaone-platforms-confirmed-full-interoperability/) completion of interoperability testing between PortaOne's PortaBilling Business Support System (BSS) and PROTEI's Home Location Register HLR/HSS and Policy Controller PCRF products.

As noted above, emails we reviewed included correspondence between Telinsol, PROTEI Russia, and Ariantel, where the parties are discussing the possibility of the "PROTEI training team" flying to Iran for a training on the instruction of Ariantel. As noted, Telinsol's director, Mr. Eskandari, is asked by Ariantel to arrange this trip.

From: Nima Eskandari [mailto:nima@telinsol.co.uk]
Sent: Wednesday, April 28, 2021 2:21 AM
To: Artur Mikhailov <mikhailov@protei.ru>; Moein Mirmoeini <Moein.m@ariantel.ir>
Cc: rasool alipour <r.alipour@ariantel.ir>; kamran baratnejad <kamran.b@ariantel.ir>; Фрейнкман Володя <vf@protei.ru>
Subject: Re: Protei Training

Hi Artur

Thank you for your email.

ArianTel would like to have the course material before attending the course. Would it be possible to share it with us?

@Moein
Moein jan Protei can not accommodate ArianTel visit to Russia due to the current Covid situation and restrictions in Russia, and as you are keen to start training I would suggest to go with online training.

Best Regards,

Nima Eskandari MBCS - Managing Director
TELINSOL LTD
73 Maple Road
Surbiton
KT6 4AG
United Kingdom
Mobile: +44 7447433823
Office: +44 2032909656

The information in this email is confidential and solely for the use of the intended recipient(s). If you receive this email in error, please notify the sender and delete the email from your system immediately. In such circumstances, you must not make any use of the email or its contents. Views expressed by an individual in this email do not necessarily reflect the opinions of Telinsol Ltd.

Telinsol Ltd.
Registered office: 73 Maple Road, Surbiton, United Kingdom, KT6 4AG. Registered in England.
Registered number: 09576707.

On 27 Apr 2021, at 20:53, Artur Mikhailov <mikhailov@protei.ru> wrote:

Hello

As the UAT tests are passed we can move for the next step - the training.
The trainers calendar is quite busy, please let me know if the following dates are suitable for you.

DPI(PCEF)	17.05-19.05
PCRF	24.05-25.05
GGSN/PGW	31.05 - 01.06
STP/DRA	07.06-08.06
SCP	09.06
SMSC+SCL	14.06
HLR/HSS	15.06-16.06
SB	21.06
RBT	23.06
VoiceMail/MCA	28.06

Kind regards,
Artur Mikhailov
Mobile: +7 (921) 845-49-25
E-mail: mikhailov@protei.ru
www.protei.com

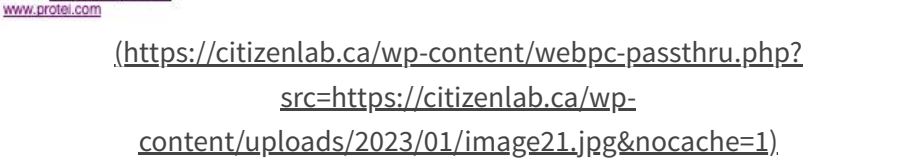
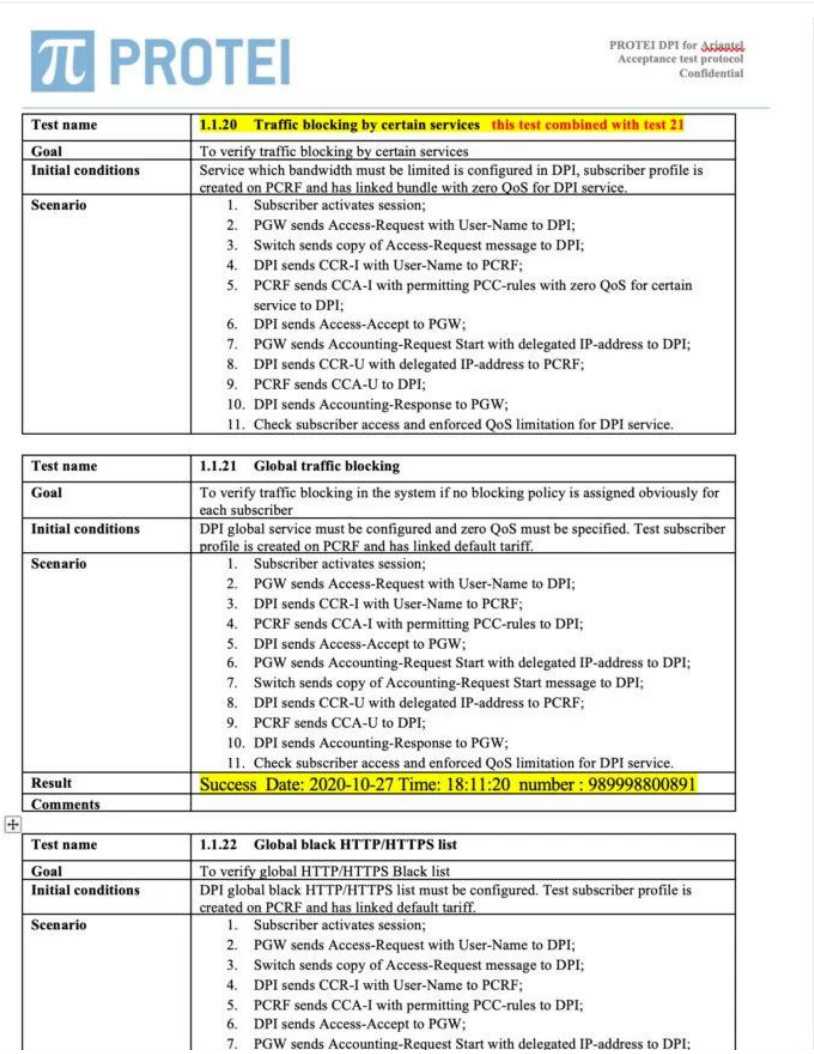

(https://citizenlab.ca/wp-content/webpc-passthru.php?src=https://citizenlab.ca/wp-content/uploads/2023/01/image21.jpg&nocache=1)

Figure 15. Screenshot of an email dialogue between PROTEI and Nima Eskandari regarding training after the completion of PROTEI User Acceptance Testing (UAT) for Ariantel



PROTEI DPI for Ariantel
Acceptance test protocol
Confidential

Test name	1.1.20 Traffic blocking by certain services this test combined with test 21
Goal	To verify traffic blocking by certain services
Initial conditions	Service which bandwidth must be limited is configured in DPI, subscriber profile is created on PCRF and has linked bundle with zero QoS for DPI service.
Scenario	1. Subscriber activates session; 2. PGW sends Access-Request with User-Name to DPI; 3. Switch sends copy of Access-Request message to DPI; 4. DPI sends CCR-I with User-Name to PCRF; 5. PCRF sends CCA-I with permitting PCC-rules with zero QoS for certain service to DPI; 6. DPI sends Access-Accept to PGW; 7. PGW sends Accounting-Request Start with delegated IP-address to DPI; 8. DPI sends CCR-U with delegated IP-address to PCRF; 9. PCRF sends CCA-U to DPI; 10. DPI sends Accounting-Response to PGW; 11. Check subscriber access and enforced QoS limitation for DPI service.

Test name	1.1.21 Global traffic blocking
Goal	To verify traffic blocking in the system if no blocking policy is assigned obviously for each subscriber
Initial conditions	DPI global service must be configured and zero QoS must be specified. Test subscriber profile is created on PCRF and has linked default tariff.
Scenario	1. Subscriber activates session; 2. PGW sends Access-Request with User-Name to DPI; 3. DPI sends CCR-I with User-Name to PCRF; 4. PCRF sends CCA-I with permitting PCC-rules to DPI; 5. DPI sends Access-Accept to PGW; 6. PGW sends Accounting-Request Start with delegated IP-address to DPI; 7. Switch sends copy of Accounting-Request Start message to DPI; 8. DPI sends CCR-U with delegated IP-address to PCRF; 9. PCRF sends CCA-U to DPI; 10. DPI sends Accounting-Response to PGW; 11. Check subscriber access and enforced QoS limitation for DPI service.
Result	Success Date: 2020-10-27 Time: 18:11:20 number : 989998800891
Comments	

Test name	1.1.22 Global black HTTP/HTTPS list
Goal	To verify global HTTP/HTTPS Black list
Initial conditions	DPI global black HTTP/HTTPS list must be configured. Test subscriber profile is created on PCRF and has linked default tariff.
Scenario	1. Subscriber activates session; 2. PGW sends Access-Request with User-Name to DPI; 3. Switch sends copy of Access-Request message to DPI; 4. DPI sends CCR-I with User-Name to PCRF; 5. PCRF sends CCA-I with permitting PCC-rules to DPI; 6. DPI sends Access-Accept to PGW; 7. PGW sends Accounting-Request Start with delegated IP-address to DPI;

(https://citizenlab.ca/wp-content/webpc-passthru.php?src=https://citizenlab.ca/wp-content/uploads/2023/01/image14.jpg&nocache=1)

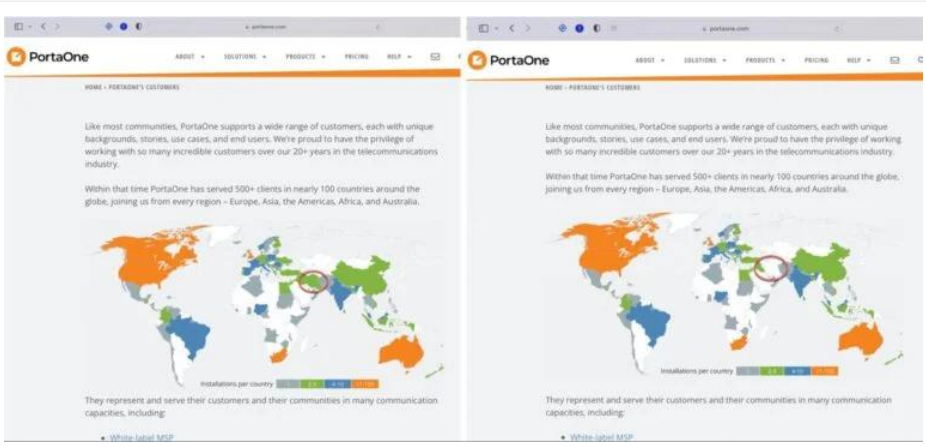
Figure 16. Screenshot of data Traffic Blocking testing results from the PROTEI DPI Acceptance Testing Protocol (ATP) document for Ariantel

PortaOne Inc.

PortaOne Inc. (https://www.portaone.com/) is a Canadian telecommunications company based (https://beta.canadasbusinessregistries.ca/search/results?search=%7Bportaone%7D&status=Active) in British Columbia and founded (https://www.portaone.com/company/) in 2001. The company has two listed directors (https://ised-isde.canada.ca/cc/lgcy/fdrlCrpDtls.html?lang=eng&corpId=4316118). Andriy Zhylenko, who has listed an address in Barcelona, Spain and is the company's CEO (https://www.portaone.com/company/leaders/), and Oleksandr Kapitanenko, the company's President (https://www.portaone.com/company/leaders/) who has listed an address in Coquitlam, BC in Canada. PortaOne supplies software for telecommunications companies (https://www.portaone.com/telecom-products/), including billing and charging platforms (PortaBilling (https://www.portaone.com/telecom-products/portabilling/)) and service management and delivery systems for voice, messaging, IoT/M2M, and data traffic (PortaSwitch (https://www.portaone.com/telecom-products/portaswitch/)), among other software solutions.[3]

On the PortaOne customer webpage (https://www.portaone.com/portaones-customers-valued-members-of-the-telecommunications-industry/), they claim to have served over 500 clients in nearly 100 countries. While they do not name Iranian customers, the PortaOne website included, prior to January 11, 2023, a colour-coded installation map that indicated the company was involved in 2-3 installations in Iran. On January 11, 2023, after we received the response from PortaOne (see Appendix C) that installation map was updated to remove the Iran installations (see

Figure 14). In a subsequent statement (also included in Appendix C), PortaOne explains that the map on their website mistakenly combined Iraq (where they have customers) with Iran (where they stated not to have customers) and that the map was subsequently corrected.



(https://citizenlab.ca/wp-content/webpc-passthru.php?src=https://citizenlab.ca/wp-content/uploads/2023/01/image5.jpg&nocache=1)

Figure 17. Screenshots of the customer installation map on the PortaOne website taken on January 10, 2023 (left) and on January 11, 2023, at 12pm Eastern (right). Circle was added to highlight Iran.

Responses from PortaOne

PortaOne provided the Citizen Lab with two responses prior to the publication of this report. On January 10, 2023, in the first response sent by their counsel, PortaOne stated that the company "does not provide any products or services to or for use in Iran, it has never done business with Iran, Telinsol or Ariantel" (see Appendix C).

On January 11, 2023, PortaOne issued an official statement contradicting the first response. In this statement, PortaOne stated that, in 2018 and 2019, a PortaOne sales manager engaged in business discussions with Ariantel, acting through Telinsol, regarding PortaOne's products. The license deal submitted by the sales manager for approval by PortaOne's management was not with Ariantel but with a Portuguese company. PortaOne explained that it did receive a single payment under the contract between PortaOne and a Portuguese company. The payment they received under this contract came from an unrelated entity, which prompted an investigation by senior management and led to the discovery that the Portuguese company was a front for Ariantel. PortaOne claims that it subsequently canceled the contract with the Portuguese company and returned the payment received.

It is hard to understand how PortaOne's senior management was not aware of the connection between the Portuguese company (which Telinsol claimed in its January 13, 2023 response to us is named "Magicalcharacter") and Ariantel and why such an investigation was not conducted by the company prior to entering into negotiations with the Portuguese company, let alone finalizing an agreement and receiving a payment. According to the email correspondence we reviewed, it was the Business Development Director at the time at PortaOne–which suggests a relatively senior position at the company–who was primarily involved in correspondence between PortaOne, Telinsol, and Ariantel. This Business Development Director was the one to request Telinsol to provide a Telinsol email to an individual who appeared to be using an Ariantel email address, and noted in that same email that, "[a]s agreed, all correspondence must be use [sic] 'Telinsol' or generic (Gmail or yahoo) email addresses" (See Figure 8).

It is also concerning that a PortaOne employee (and, in particular, a senior employee) would not have considered the adverse human rights impacts of this potential business relationship. This same Business Development Director, as well as the email address "sales@portaone.com," was copied on an email where a software manager at Ariantel appears to have specifically asked someone in sales (a certain "Alex," which is likely referring to Alexander

Zalugovskiy, Project Manager, who is also identified in the documents reviewed) at PortaOne about "the list of APIs offering required data for LI" and noting that in their "last session talks as you said it seems that it's possible for us to implement legal requirements."

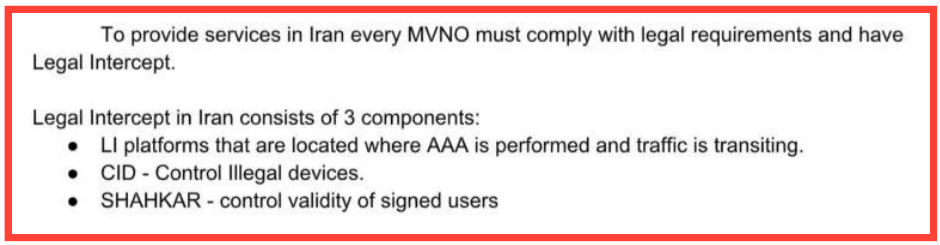
The email includes an attached document where it is specifically spelled out that "Telinsol is a Mobile Virtual Network Operator in Iran," "Telinsol is going to use Protei and PortaOne solutions to run their MVNO services," and that to provide services in Iran every MVNO "must comply with legal requirements and have Legal Intercept" which is composed of "three components. LI platforms…CID – Control Illegal devices…SHAHKAR – control validity of signed users." This summary was then followed by an extensive description of each of these Legal Intercept components (See Figures 18 and 19).


Legal Intercept

Telinsol is Mobile Virtual Network Operator in Iran. This is a totally new project and there are no running services at the moment. Telinsol is going to use Protei and PortaOne solutions to run their MVNO services.

(https://citizenlab.ca/wp-content/webpc-passthru.php?src=https://citizenlab.ca/wp-content/uploads/2023/01/image10.jpg&nocache=1)

Figure 18. Excerpt of document 'Legal Intercept for Telinsol_without_Protei_ones.docx', sent by an Ariantel "software manager" to PortaOne's Business Development Director and sales@portaone.com


To provide services in Iran every MVNO must comply with legal requirements and have Legal Intercept.

Legal Intercept in Iran consists of 3 components:

- LI platforms that are located where AAA is performed and traffic is transiting.
- CID - Control Illegal devices.
- SHAHKAR - control validity of signed users

(https://citizenlab.ca/wp-content/webpc-passthru.php?src=https://citizenlab.ca/wp-content/uploads/2023/01/image15.jpg&nocache=1)

Figure 19. Excerpt of document 'Legal Intercept for Telinsol_without_Protei_ones.docx', sent by an Ariantel "software manager" to PortaOne's Business Development Director and sales@portaone.com

Our review of the documents has not identified any exchanges with a Portuguese company or a company called Magicalcharacter acting on behalf of Ariantel. PortaOne's public statement claims that a sales manager "on his own initiative, engaged in business discussions with Ariantel, acting through Telesol [sic]". However, according to the email correspondence we have reviewed, PortaOne's Business Development Director at the time was involved in direct correspondence with at least one individual using an Ariantel email address. As noted above, a document sent to two PortaOne email addresses included direct references to the proposed project involving an MVNO operating in Iran.

A set of documents that appear to have been prepared or edited by a project manager at PortaOne illustrate that at least two PortaOne employees were aware that the proposed project with Telinsol involved providing services to an Iran-based MVNO. In a document describing various features of the services PortaOne would provide to Telinsol,

comments attributed to a 'Alex Zalugovskiy' at PortaOne make multiple references to components of the project requiring CRA approval. A set of documents from August 2019 that are described as having been prepared by 'Alexander Zalugovskiy', described as a 'project manager' at PortaOne, indicate that the proposed project with Telinsol required Farsi language support, as well as support for the Jalali calendar used in Iran. Together, the documents indicate that at least two employees of PortaOne were aware, or had reason to be aware, that the proposed project with Telinsol involved providing services to an Iran-based MVNO.

In sum, PortaOne's communications to us have evolved from a blanket denial to an admission that some business was conducted and then subsequently investigated and closed down. However, the information contained in the documents we reviewed does not fully align with their explanation, nor does it demonstrate the type of due diligence they claim to follow.

Conclusion

The documents reviewed in this report provide a glimpse into the Iranian government's attempt to build a comprehensive surveillance regime and the role of foreign entities in potentially facilitating that system. While we cannot say whether the surveillance system in question was fully or partially implemented, as we only have insight into a moment in time, these documents clearly do reflect an aspiration for an unprecedented surveillance architecture that would have–based on the Iranian regime's history of suppressing dissent and human rights–led to further human rights violations. Further research is required to understand whether, and to what extent, this system was fully developed and if so, by whom.

In addition, the documents clearly show that several foreign firms were actively negotiating[4] to provide services and technology that our analysis suggests would have helped facilitate the Iranian regime's legal intercept capabilities. In addition to respecting domestic law (such as sanctions regimes), under the framework (https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf) of the *United Nations Guiding Principles on Business and Human Rights* (UNGPs), corporate actors have a responsibility to respect human rights and seek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts. While businesses may argue that their services are innocuous and not specifically designed for legal interception, this does not absolve them of the responsibility to undertake a human rights due diligence process (https://www.bsr.org/reports/BSR-Human-Rights-Due-Diligence-Products-Services.pdf) to identify, prevent, mitigate, and account for how they will address adverse human rights impacts in the context of a potential client.

Further, in this case, the correspondence exchanged by the parties should have put the foreign companies on notice that their products could be integrated into a broad legal intercept architecture being operated by a government with a notoriously poor human rights record. As one example, in email discussions regarding the project exchanged between Ariantel and PortaOne in June 2019, Ariantel provided CRA Legal Intercept requirements, outlining the extent to which Iranian authorities required visibility into, and control of, user mobile services. Citizen Lab's research into the email communications and documentation shared with vendors provide unmistakable clarity into the intentions of the Iranian regime with regard to regulations over mobile operator services.

UN Special Rapporteurs (https://freedex.org/wp-content/blogs.dir/2015/files/2017/05/AHRC3522.pdf), governments (https://www.ihrb.org/pdf/eu-sector-guidance/EC-Guides/ICT/EC-Guide_ICT.pdf), multi-stakeholder platforms (https://globalnetworkinitiative.org/gni-provides-input-david-kaye/), and telecommunications industry leaders (https://www.ericsson.com/en/about-us/sustainability-and-corporate-responsibility/responsible-business/human-rights) have all recognized the significant impact (https://www.ohchr.org/sites/default/files/Documents/Issues/Expression/Telecommunications/Article19.pdf) of telecommunications products and services on freedom of expression and privacy (https://documents-dds-ny.un.org/doc/UNDOC/GEN/G16/095/12/PDF/G1609512.pdf?OpenElement), and have emphasized the need to im-

plement such human rights assessment procedures. None of the companies who provided a response to this report have offered concrete information regarding having such a human rights due diligence process in place prior to engaging in business with new clients. In particular, PortaOne's second response to the Citizen Lab raises serious questions regarding how the company vets clients for risks of adverse human rights impacts (as well as potential sanctions violations), what oversight is exercised by senior management, and what measures exist to ensure that similar situations do not arise in the future.

Acknowledgements. We are grateful to Siena Anstis, Jakub Dalek and Bill Marczak for internal review, Mari Zhou for graphics, and Snigdha Basu for copy editing.

Appendix A. Documents Reviewed

The following table lists the documents included as attachments in email communications shared with the Citizen Lab for analysis by *The Intercept*.

Date and Subject of Email	Email Recipient Domains
August 7, 2021 Siam Document	• cra.ir • ariantel.ir
May 2, 2020 Shahkar-Estelam-Document	• cra.ir • ariantel.ir
September 21, 2019 FW. Purchase Order PO-1151/ PO-0030 from Telinsol Ltd for VALID Middle East FZE	• ariantel.ir • Includes Forwarded Email from valid.com
September 1, 2019 مستندات درخواستی English Translation "Requested documents"	• ariantel.ir • bahar.network (Name Servers Operated by
August 18, 2019 Contract material with Porta One	• ariantel.ir

Date and Subject of Email	Email Recipient Domains
August 28, 2019 Final Agreement between Telinsol and Porta One	• telinsol.co.uk • ariantel.ir
June 21, 2019 PortaOne Converged BSS-OSS and Billing for Telinsol in UK	• portaone.com • ariantel.ir • telinsol.co.uk • gmail.com • yahoo.com
June 11, 2019 RE. APIs supporting Legal Intercept	• ariantel.ir • portaone.com
April 28, 2019 Li& shahkar& CID	• ariantel.ir
July 12, 2021 Re: Protei Training	• telinsol.co.uk • protei.ru • ariantel.ir

Appendix B. Glossary

The following glossary includes a contextual list of specialized terms and acronyms used in this report.

- **Access Point Name (APN)** A name configured in the device and network which specifies the type of network data connection assigned to a user, such as an MVNO or other private mobile network.
- **Business Support System (BSS)** A software function responsible for storing information about mobile service provider products, rates, customers, customer information, or phone lines. It enables customer billing and controls service configuration and activation.
- **Credit-Control-Answer (CCA)** A command response from a PCRF used to provision rules and triggers to control a user data session, such as bandwidth limiting or data blocking.

- **Credit-Control-Request (CCR)** A command sent to a PCRF used to request rules to issue user data session controls, such as bandwidth limiting or data blocking.
- **Call Detail Record (CDR)** Provides detailed information about user voice calls or SMS messages including time, duration, location, source, and destination number.
- **Deep Packet Inspection (DPI)** An in-line software network function used by mobile service providers that receives and processes user data information, detects and classifies it into service types, and enables controls such as blocking, bandwidth restriction, and deep analysis.
- **Home Location Register/Subscriber Server (HLR/HSS)** A software network function that supports user mobile services including authentication, authorization, status, and communication with other network functions to enable voice, data, and messaging services.
- **Internet Protocol Detail Record (IPDR)** Provides detailed information about user data sessions including time, location, server IP address, data volume, service identification, protocol, subscriber identifier.
- **Mobile Virtual Network Operator (MVNO)** A mobile service provider that sells services under its brand name but uses the radio network of another licensed mobile operator.
- **Policy and Charging Rules Function (PCRF)** A software function used for receiving and activating rules for controlling a user data session.
- **Packet Data Network Gateway (PGW)** A software network function that routes and filters user data from the mobile network to external networks such as the Internet.
- **Quality of Service (QoS)** A description commonly associated with the amount of network bandwidth available to a user's mobile data services.
- **Short Message Center (SMSC)** A software network function that stores and forwards SMS messages.
- **Unstructured Supplementary Service Data (USSD)** An interactive legacy mobile messaging protocol commonly used in mobile networks for basic applications such as order confirmation, mobile account payments, and short surveys.

Appendix C. Correspondence with Companies[5]

PortaOne

▶ ***January 4 2023 – Letter sent from Citizen Lab to PortaOne (https://citizenlab.ca/wp-content/uploads/2023/01/PortaOne_January-4-2023.pdf)***
▶ ***January 11 2023 – Email sent from PortaOne (via Fraser Litigation Group) to Citizen Lab (https://citizenlab.ca/wp-content/uploads/2023/01/PortaOnetoCL_January112023.pdf)***
▶ ***January 11 2023 – Public statement from PortaOne (https://citizenlab.ca/wp-content/uploads/2023/01/PortaOne_OfficialStatement_January-112023.pdf)***
▶ ***January 12 2023 – Letter sent from Citizen Lab (via Palaire Roland) to PortaOne (via Fraser Litigation Group) (https://citizenlab.ca/wp-content/uploads/2023/01/CLtoPortaOne_January-122023.pdf)***
▶ ***January 13 2023 – Letter from PortaOne (via Fraser Litigation Group) to Citizen Lab (https://citizenlab.ca/wp-content/uploads/2023/01/PortaOnetoCL_January132023-1.pdf)***[6]

Telinsol

▶ ***January 4 2023 – Letter sent from Citizen Lab to Telinsol (https://citizenlab.ca/wp-content/uploads/2023/01/Telinsol_January-4-2023.pdf)***
▶ ***January 11 2023 – Letter from Telinsol (via DLA Piper) to Citizen Lab (https://citizenlab.ca/wp-content/uploads/2023/01/TelinsoltoCL_January-112023.pdf)***

▶ ***January 13 2023 – Letter from Telinsol (via DLA Piper) to Citizen Lab (https://citizenlab.ca/wp-content/uploads/2023/01/TelinsoltoCL_January132023.pdf)***

▶ ***January 14 2023: Letter from Citizen Lab to Telinsol (https://citizenlab.ca/wp-content/uploads/2023/01/CLtoTelinsol-January142023.pdf)***

PROTEI

▶ ***January 4 2023 – Letter from Citizen Lab to PROTEI (https://citizenlab.ca/wp-content/uploads/2023/01/PROTEI_January-4-2023.pdf)***

---

1. The document also notes that "[t]his is a totally new project and there are no running services at the moment."↩
2. Infrastructure search engines Censys and Shodan showed fingerprints of PROTEI equipment present in Kazakhstan, Uzbekistan, and Russia when searched on 2022-11-30, and showed as an equipment vendor in Jordan, Kyrgyzstan, Uzbekistan, and Tajikistan based on RAEX IR.21 reporting data.↩
3. PortaOne maintains a public wiki that includes discussions (https://wiki.portaone.com/display/REQSPEC/Routing+On-Net+Calls+to+Vendors) around compliance with lawful intercept requirements worldwide, including a 2017 discussion (https://wiki.portaone.com/pages/viewpage.action?pageId=60950236) on compliance with Russia's SORM (System for Operative Investigative Activities) system.↩
4. Note that in PortaOne's second response to the Citizen Lab (see Appendix C), the company explains that it did contract with a Portuguese company and, under this contract, received a single payment from an unrelated entity. This payment prompted an investigation by senior management and led to the discovery that the Portuguese company was a front for Ariantel.↩
5. Formatting for this section was updated on January 18th, 2023.↩
6. This letter was added after publication on January 16th, 2023.↩

Privacy Policy (https://citizenlab.ca/privacy/)

Unless otherwise noted this site and its contents are licensed under a Creative Commons Attribution 2.5 Canada (https://creativecommons.org/licenses/by/2.5/ca/) license.

munkschool OF GLOBAL AFFAIRS & PUBLIC POLICY UNIVERSITY OF TORONTO

(http://munkschool.utoronto.ca/)