TU WIEN Informatics

Zero-Rating, One Big Mess

Analyzing Differential Pricing Practices of European Mobile Network Operators

DIPLOMARBEIT

zur Erlangung des akademischen Grades

Diplom-Ingenieur

im Rahmen des Studiums

Software Engineering & Internet Computing

eingereicht von

Gabriel Karl Gegenhuber, BSc
Matrikelnummer 01327045

an der Fakultät für Informatik

der Technischen Universität Wien

Betreuung: Univ.-Prof. Dipl.-Ing. Mag. Dr. techn. Edgar Weippl
Mitwirkung: Dipl.-Ing. Wilfried Mayer

Wien, 13. Oktober 2021

Gabriel Karl Gegenhuber	Edgar Weippl

TU WIEN Informatics

Zero-Rating, One Big Mess

Analyzing Differential Pricing Practices of European Mobile Network Operators

DIPLOMA THESIS

submitted in partial fulfillment of the requirements for the degree of

Diplom-Ingenieur

in

Software Engineering & Internet Computing

by

Gabriel Karl Gegenhuber, BSc
Registration Number 01327045

to the Faculty of Informatics

at the TU Wien

Advisor: Univ.-Prof. Dipl.-Ing. Mag. Dr. techn. Edgar Weippl
Assistance: Dipl.-Ing. Wilfried Mayer

Vienna, 13th October, 2021

Gabriel Karl Gegenhuber	Edgar Weippl

Technische Universität Wien
A-1040 Wien ▪ Karlsplatz 13 ▪ Tel. +43-1-58801-0 ▪ www.tuwien.at

Erklärung zur Verfassung der Arbeit

Gabriel Karl Gegenhuber, BSc

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit – einschließlich Tabellen, Karten und Abbildungen –, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.

Wien, 13. Oktober 2021

Gabriel Karl Gegenhuber

Acknowledgements

I would like to thank my co-advisor Wilfried for the support and valuable feedback throughout my thesis. He was always there to help, providing special expertise regarding maps, bathtubs, and soccer fields. Moreover, I want to thank SBA Research, the netidee funding program, the TU Vienna, and NLnet for funding and supporting my work. Likewise, I want to thank all the volunteers for hosting a MobileAtlas probe which enabled the measurements I collected for this study. Furthermore, I am grateful for my friends, colleagues, and my girlfriend, who gave me moral support and motivation when I needed it. A special thank goes out to Stefan, who always was a faithful companion during my time at university. Finally, I would like to thank my parents, Eva and Karl, for providing financial support during my studies and giving me the freedom to chose my own path. Without them, I would not be where I am today. Thank you.

Kurzfassung

Spätestens seit der Abschaffung der Roaminggebühren im EU-Raum ist Mobilfunk nicht nur national, sondern auch auf Reisen eine der wichtigsten Internet-Zugangstechnologien. Unabhängig davon bieten immer mehr europäische Mobilfunkbetreiber Tarife mit Zero-Rating an. Obwohl Roaming und Zero-Rating wesentliche konsumentenschutzrechtliche Auswirkungen haben können, gibt es kaum Einblick in gängige Praktiken und keine geeigneten Werkzeuge um Provider kontrollieren zu können. Existierende Internet-Messplattformen wurden für traditionelle Festnetzanschlüsse entworfen und sind für mobiles Internet aufgrund unterschiedlicher Anforderungen (z.B. begrenztes Datenguthaben, Datenroaming, Zero-Rating, etc.) nur bedingt geeignet. Deshalb stellen wir mit MobileAtlas eine neue Messplattform für Mobilfunknetze vor, die sich dieser Lücke annimmt. MobileAtlas ermöglicht es lokale SIM-Karten übers Internet zu tunneln und auf einer Messstation im Zielland zu emulieren. Die geographische Entkopplung von SIM-Karte und Modem ermöglicht somit das Durchführen von Roaming-Messungen ohne physisch ins Ausland reisen zu müssen. Neben guten Skalierungseigenschaften bei internationalen Messungen bietet die Plattform außerdem eine vollständig isolierte Messumgebung, in der auch kleine Datenströme gemessen und protokolliert werden können. Wir verwenden MobileAtlas, um Zero-Rating bei sieben Mobilfunkanbietern in drei verschiedenen europäischen Ländern zu untersuchen und evaluieren. Dazu führen wir mehr als 200 Messungen in heimischen Mobilfunknetzten, sowie in internationalen Roaming-Umgebungen durch und identifizieren potenziell problematische Praktiken bei mehr als der Hälfte der untersuchten Mobilfunktarifen. Zusammen mit den Ergebnissen unserer europäischen Marktanalyse bietet diese Arbeit einen gut strukturierten Überblick über die europäische Zero-Rating-Landschaft und hilft dabei detailliertere Einblicke in gängige Providerpraktiken zu erhalten.

Abstract

Mobile cellular networks have become a major access technology to the public Internet. While roaming was expensive and sparsely used in the early days, free roaming agreements such as in the European Union have erased borders for end customers and let them perceive cellular service in an international and unified fashion. In addition, new tariff models that introduced zero-rating, where data of certain applications does not count towards a customers' bill, have appeared within the mobile ecosystem. Roaming and zero-rating are significant to consumer protection and net neutrality. However, there is little insight into current practices and a lack of tools to independently audit network operators. To fill this gap, we introduce the MobileAtlas measurement platform. MobileAtlas is an open and extensible platform that focuses on fine-grained measurements and geographically decouples the SIM card from the cellular modem by tunneling the corresponding communication protocol over the Internet. Thus, it enables taking roaming measurements in a well scalable manner. We use the framework to analyze zero-rating at seven providers within three different European countries. We execute and evaluate more than 200 measurements within domestic and internationally roamed environments and identify potentially problematic practices at more than half of the investigated providers. Together with the results of our European market analysis, we provide a structured overview of the European zero-rating landscape and help to get more detailed insights into current provider practices.

Contents

CHAPTER 1

Introduction

Mobile cellular networks have become a major access technology to the public Internet. Worldwide mobile data traffic has just surpassed the share of desktop traffic and is still on the rise [1].

Besides the obvious technical differences between mobile broadband and landline Internet access, there is also a huge difference in how and under which restraints they're utilized. While fixed-line access is restricted to a single location, Smartphones are constant companions in our everyday life, and the ubiquitous use of data roaming has made us even more reliable on this technology. Last but not least, they also differ in economic nature. Fixed-line offers usually provide unlimited data volume, whereas mobile broadband connections are metered and often use complex billing schemes.

In June 2017, the European Union abolished data roaming fees for the intra-EU/EEA area under the "roam like at home" doctrine. This regulation made roaming in foreign cellular networks feel and behave like at the home operator and led to a drastic increase in roaming traffic [2].

According to BEREC [3], a growing number of Mobile Network Operators (MNOs) have introduced differential pricing (e.g., zero-rating) offers, and some of them have already been caught disrespecting network neutrality principles during international data roaming [4, 5]. Possibly, many net neutrality violations remain undiscovered, and proving a provider's misbehavior is not easily possible. Often there is anecdotal evidence, i.e., a customer observes wrongfully billed traffic after spending their vacation abroad, but there is no way of actually proving the mobile provider violated their contract. Of course, a customer that feels unfairly treated can always report the issue to the corresponding National Regulatory Authority (NRA). NRAs are responsible for supervising their country's providers and take action when contract or basic net neutrality violations are discovered. However, even an NRA cannot easily decide whether a customer's complaint against a provider is legitimate or not. To be sure, they would have to obtain the same

product as the complaining customer and re-enact the situation, which means they'd need to travel to the target country when roaming is involved. Obviously, this is not feasible since it would require exceedingly high cost and coordination effort from the NRA. Often, the NRA just asks the provider for more precise data on the incident and then mediates between the complaining customer and the provider until a satisfactory solution for both parties has been found. While this is good for the involved customer, since it strengthens the negotiating position against the provider, who usually has a lot more available resources than its customers, it does not solve the initial problem. Furthermore, due to complex tariff structures (especially within zero-rating offers), not-so-tech-savvy customers might not even notice wrongfully billed units and just pay the bill. Supposedly, sometimes even providers don't fully comprehend the tariffs they're offering or at least do not consider the consequences of promises that were made within special tariffs (e.g., zero-rating all traffic caused by one app) and thus violate their contracts unintentionally. Besides violating net neutrality in an economic sense, providers should also be checked for technical (e.g., when throttling specific traffic) and privacy-related violations. Within zero-rating offers, many providers use deep packet inspection to classify a customer's data traffic. Obviously, inspecting a user's data packets up to the application layer can be privacy-invasive and, therefore, should be monitored and supervised precisely. Sadly, in most cases, we do not have any information on how those classifiers work and what actually happens behind the curtain. Being able to have a third party monitor a customer's data traffic and the corresponding billing units, not only for domestic use but also in roaming environments, is a lacking skill that is needed to reliable supervise the providers and not leave this task in the hands of vigilant customers. With this ability, one could detect even small errors in a provider's billing mechanisms and therefore confirm or disprove a customer's claim of malfunctioning billing. Furthermore, providers could also use this to prove the correctness of their billing mechanisms and legitimate their tariffs. Although there is a rich set of internet measurement tools and platforms, most of them target fixed-line connections and do not fit the requirements that are needed to take measurements in the cellular field. Few scientific studies have been conducted on measuring mobile broadband in roaming environments. The complex ecosystem drives up the cost and coordination effort that is necessary to orchestrate international measurements. For example, in one of the biggest roaming studies [6], they measured 16 providers in 6 countries and therefore had to acquire 6 SIM cards of every provider (one for each country). SIM cards had to be manually changed, which was coordinated via email. Although this might work for smaller studies, it has a considerable coordination overhead and scales not very well for a bigger number of countries and providers (since one SIM card per country and provider is needed).

The research questions of this thesis are centered around investigating whether billing mechanisms of mobile network providers within the EU work properly and respect net neutrality principles, with a particular focus on zero-rating offers and roaming inside other EU countries. More specifically, this thesis seeks to contribute to a better understanding of state-of-the-art traffic classification mechanisms and tries to identify common metrics that are used to classify data traffic.

To address the gap we identified in current measurement platforms and to solve the problems that are mentioned above, we introduce the MobileAtlas measurement platform. MobileAtlas implements an approach to geographically decouple the SIM card and modem, which boosts the scalability and flexibility of mobile network measurements. More specifically, our measurement platform allows a local SIM card to be virtually connected to a remote modem in another country without physically moving any hardware between different countries. This fundamentally reduces the required coordination effort and changes the scaling behavior of mobile network measurements since one SIM card can be measured in an arbitrarily high number of countries without any physical intervention needed. We believe that our platform finally makes international large-scale mobile network measurements feasible. Furthermore, MobileAtlas offers an isolated measurement environment that is fully controlled by the test operator, which makes it perfectly suitable for billing-wise measurements of small payloads.

In conclusion, the scientific contribution of this thesis is:

- We structured the problematic and chaotic ecosystem at mobile network providers and investigated the tariffs that are currently available.
- We found a gap of capabilities that are not supported within current mobile network measurement platforms.
- We developed an international measurement platform that makes large-scale mobile network measurements feasible.
- We used this platform to measure seven SIM cards that come from three different countries in eight different target countries.
- We examined billing mechanisms deployed within zero-rating offers during domestic and roaming usage scenarios.
- We found questionable behavior at multiple providers.

The remainder of this thesis is structured as follows. In Chapter 2, we introduce some basic concepts that are relevant to this thesis. Chapter 3 gives an overview of other studies that were similar to this work. In Chapter 4, we describe our methodological approach and introduce the MobileAtlas measurement platform. In Chapter 5 the results of this study are presented. Finally, we discuss the results in Chapter 6 and make a conclusion in Chapter 7.

CHAPTER 2

Background

This chapter describes some basic concepts that are relevant to this thesis. Because the required background touches various aspects in different fields, we structured it into four sections. While Section 2.1 and Section 2.2 describe cellular and Internet technologies, Section 2.3 outlines some fundamental net neutrality and traffic classification concepts. Finally, we conclude with Section 2.4 by providing a brief introduction to the most important open-source projects that were utilized during this thesis.

2.1 Cellular Technologies

While the first commercial digital cellular network (2G) was deployed in the early 90s and new generations that provide enhancements have been released about every tenth year, many fundamental concepts are still similar to the early days.

2.1.1 (U)SIM card

A Subscriber Identity Module (SIM) is an integrated circuit card containing cryptographic material and identifies the user to a specific mobile network. It was introduced in GSM and was later renamed to Universal Subscriber Identity Module (USIM) for UMTS and LTE. (U)SIM cards decouple handset manufacturers from network operators and are used to authenticate and authorize the user to the mobile network by containing a secret key that is pre-shared with the network operator. Because the COMP-128 algorithm that was used for authentication in earlier SIM cards was shown to be cryptographically flawed, newer cards use the AES-based MILENAGE algorithm instead. The communication between the handset and the SIM card is based on Application Protocol Data Units (APDUs) and was standardized by ISO/IEC 7816-4.

2.1.2 Modem Protocols

When plugging a modem dongle into a computer system, different protocols may be offered by the modem for interaction. Traditionally, a modem would expose one or more serial devices, reacting to AT-commands that are sent by the system. Although modem manufacturers seem to agree on a basic subset of commands, many modems implement proprietary commands or even deviate from the norm. When establishing a network connection via the modem, the serial interface is also used to transfer data (via PPP) between the modem and the system. This introduces an unnecessary overhead because all data packets have to be wrapped inside PPP packets. Because newer radio protocols like LTE have native support for IP packets, Qualcomm MSM Interface (QMI), and Mobile Broadband Interface Model (MBIM) have been introduced. When using QMI or MBIM, the modem exposes multiple different devices to the system and separates the network interface from the command and control access.

2.1.3 Roaming Models

There are three approaches to how data connections are routed during roaming: Home-Routed Roaming (HR), Local Breakout (LR), and IPX Hub Breakout (IHBO). When HR is used, the roamed device obtains its IP address from its home operator, and all data traffic that occurs within the roamed connection is routed over a tunnel to the home network. This is the most common approach that is currently used by the majority of European operators. In case of LR, the roamed device gets an IP address from the visited network, and the data traffic is directly routed to its destination without taking a detour over the home operator. Finally, IHBO is a more recent approach, where the connection is terminated by a third party somewhere between the visited and the home network.

2.2 Internet Protocols

This section briefly describes some aspects of Internet protocols that are relevant for traffic classification.

2.2.1 IP

The Internet Protocol (IP) operates at the network layer and is responsible for relaying data packets from the source host to the destination host. Therefore it provides an addressing system for network host interfaces and enables dynamic routing of data packets. Furthermore, it defines the structure of a data packet that consists of header and payload and implements mechanisms for encapsulation and fragmentation of data packets. The packet header contains all relevant data that is needed for routing a packet from the source to the destination. While the first major version (IPv4) of the protocol is still dominant on the public Internet, an upgraded version (IPv6) that increases the amount of available addresses has been released and is already growingly deployed in the wild (current adoption is about 30% [7]).

2.2.2 HTTP

The Hypertext Transfer Protocol (HTTP) is one of the most used Internet protocols and a fundamental building block of the World Wide Web. It operates at the application layer and defines a response-reply based client-server model, where the client (e.g., a web browser) sends an HTTP request to the server, which is answered with an HTTP response by the server. Although it was originally developed to request static resources from remote locations, nowadays, servers often answer with dynamically created content. Furthermore, it plays a fundamental role in machine-to-machine communication (e.g., via REST).

Because the HTTP protocol did not provide any encryption, the HTTP Secure (HTTPS) extension was introduced. Before transmitting the actual payload, the client establishes an encrypted channel (usually via TLS) to the server. Subsequently, the request-response pair is transmitted over the encrypted channel. This is not only a huge improvement in terms of privacy but also provides authentication of the accessed website and ensures the integrity of the exchanged data, because HTTPS requires the server to provide a digital certificate that can be verified by the client. Therefore, it also protects against man-in-the-middle attacks (e.g., eavesdropping, tampering).

While HTTP/1 was revised by HTTP/2 that provided several performance improvements (e.g., better compression, multiplexed connection), both HTTP/1 and HTTP/2 are based on TCP connections. HTTP/3 differs fundamentally because it relies on QUIC and therefore uses the connectionless UDP protocol.

2.3 Network Neutrality

Network neutrality (commonly abbreviated as "net neutrality") defines the principle that Internet Service Providers (ISPs) have to treat all (legal) data traffic equally. It aims to protect the open Internet by ensuring that ISPs do not block, slow down or charge differently for specific online content. Without net neutrality, established companies may pay ISPs to receive special treatment (e.g., prioritizing their traffic in so-called "fast-lanes") or to throttle or block websites and services of smaller competitors. Therefore, net neutrality supports innovation instead of monopolization by ensuring that customers may unaffectedly decide which services they want to use.

2.3.1 Differential Pricing and Zero-Rating

Differential pricing is traffic differentiation in an economical manner, i.e., when a provider, or more specifically a provider's data tariff, applies different prices for data packets from specific applications or companies. The most prominent example of differential pricing is zero-rating, which is the practice of providing access to particular services at zero cost. Data packets that meet the tariffs zero-rating criteria do not count towards a users' data cap, while unaffected data packets are normally billed.

2.3.2 Classifier Metrics

In this section, we give a short overview of so-called "signatures" [8] that are commonly used by providers to fingerprint their data packets and determine the corresponding service or application.

TCP/UDP Port. The simplest metric that can be used for classification is the port number inside the TCP or UDP header. Common internet protocols are usually assigned to a well-known port (e.g., 443 for HTTPS). While the port can therefore be used to defer the used protocol, it is usually not exclusive to a specific application or service (since other services might also use HTTPS for transmission). Some protocols use random port numbers, and applications may be re-configured to deviate from the default port, thus leading to wrong classifications. To increase reliability, this approach is usually combined with other metrics (e.g., IP address).

IP Address. While IP addresses on the client-side tend to be short-lived, randomly assigned, or even shared (e.g., carrier-grade NAT), addresses on the server-side usually are rather static. Since the IP address is easily available in the IP packet header, it is a popular classification metric. Although an application usually establishes connections to many different endpoints, those addresses can still be easily assigned to an application or company because they are typically sold or rented in big blocks. However, content delivery networks may serve a large number of sites or applications at once, which might lead to wrong classification. Furthermore, the addresses that correspond to a certain application might change over time when a company migrates a service to a different server, making it cumbersome to keep the mapping up to date.

TTL. The IP protocol implements a Time To Live (TTL) field that limits the lifespan of a data packet and prevents it from circulating indefinitely, thus clogging the network. The field is set to an initial value (e.g., 64) by the sender and is decremented by every hop that processes the data packet. When the counter reaches zero, the packet is marked as undeliverable and is discarded. Modern smartphones usually provide a tethering functionality that allows sharing the Internet connection with other devices (e.g., via USB, Bluetooth, or Wi-Fi). When the smartphone relays data packets that originate from connected devices, it decrements the TTL field accordingly. Therefore, these packets contain a different TTL value when they are processed by the provider. Furthermore, different operating systems use different initial values for the TTL field, which allows device fingerprinting and makes it even more obvious that a tethered connection was used. Therefore, providers often use the TTL value to detect and differentiate tethered data traffic.

Deep Packet and Hostname Inspection. As the name suggests, Deep Packet Inspection (DPI) does not only look at a packet at the network or transport layer, but inspects user data that may go up to the application layer. In unencrypted protocols, such as HTTP, the classifier might decide based on the Host-Header or just look for a regular expression that is known to be present in certain services. However, in encrypted

protocols (i.e., HTTPS), the desired content is unavailable to the classifier. Nevertheless, when TLS is used for encryption, the client sends a Server Name Identification (SNI) along with the initial handshake. Because the SNI address usually corresponds with the hostname, this is often used for classification. Note that newer TLS versions introduce an Encrypted SNI (ESNI) that prevents hostname inspection and hinders this classification approach.

2.4 Open-Source Software

The following open-source projects were helpful for creating this thesis.

2.4.1 Ansible[1]

Ansible is a tool that is used for configuration management, software provisioning, and application deployment for large infrastructure. Instead of manually deploying one and the same thing to many different endpoints, the desired deployment is expressed in a configuration file and can then automatically be rolled out to multiple targets. Ansible depends on Python, and for configuration YAML files are used. To access the managed targets, it typically connects via SSH.

2.4.2 WireGuard[2]

WireGuard is a lightweight and encrypted VPN protocol. It aims to outperform traditional VPN protocols (e.g., OpenVPN and IPsec) in terms of usability, high-speed performance, and flexibility (e.g., by supporting various network topologies). It operates on layer three and uses UDP sockets for communication between peers. Each peer has its own generated key pair, and the corresponding public key needs to be pre-shared with other peers when adding a new node to the network. Although it was initially implemented for the Linux kernel, nowadays, there are open source implementations for a broad range of platforms (e.g., Windows, macOS, Android).

2.4.3 pySim[3]

pySim is written in Python and is a powerful tool that is used to interact with SIM cards. It implements SIM card communication for various SIM card readers (e.g., PCSC-reader, serial/UART-based-reader), and its original purpose was to be used to provision programmable SIM cards (when running your own cellular network).

[1] https://www.ansible.com/
[2] https://www.wireguard.com/
[3] https://github.com/osmocom/pysim

2.4.4 Linux Namespaces

Linux namespaces allow to isolate kernel resources and limit them to a certain set of processes. Ever since the big success of Docker, containerization and sandboxing are well-known concepts in modern software architecture. Those concepts are usually built upon Linux namespaces. Each process (or process-group) is associated with one namespace and therefore only has access to the resources that are associated with the corresponding namespace. There are various namespace types for different resources: mount, process-id, interprocess-communication, uts, user-id, cgroup, time.

2.4.5 NetworkManager

NetworkManager is a software package that provides an interface to manage the network configuration. It is used by almost all Linux distributions. While the daemon is accessible via D-Bus, the user usually interacts with the daemon by using a graphical frontend or a command-line interface (e.g., nmcli). It was particularly developed to work with dynamic environments where network interfaces change over time. Due to the diverse landscape of network interfaces, it often relies on other software to support certain devices (e.g., ModemManager to support cellular modems).

2.4.6 ModemManager

Similar to NetworkManager, ModemManager also runs as software daemon and provides an interface to manage network interfaces, specifically cellular modems. It supports modems that communicate via serial device (via AT-commands), but also more recent protocols like QMI or MBIM. Different modems often have different behavior or implement additional commands, which ModemManager tries to compensate by its plugin-based software structure. NetworkManager relies on ModemManager to configure setup the network connection of modem devices, but its functions can also be directly called via D-BUS (e.g., to query the modem's status, send an SMS or make a phone call)

2.4.7 tcpdump[4] and PCAPdroid[5]

tcpdump is a commandline tool to dump traffic on a network. PCAPdroid is a very similar tool that was specifically developed to work on Android devices. While tcpdump only offers to listen on specific network interfaces or to collect a systemwide recording of all occurred data packets, PCAPdroid supports collecting an application-based packet stream, ignoring traffic that was generated by other apps. To reach that goal, it globally intercepts all packet streams via the Android VpnService[6].

[4] https://www.tcpdump.org/
[5] https://github.com/emanuele-f/PCAPdroid
[6] https://developer.android.com/reference/android/net/VpnService

2.4.8 JADX[7]

An android app is usually represented as .apk file that contains packed .dex resources that represent the source code of the application. JADX is a decompiler that can be used to transform the compiled bytecode into human-readable Java files. Furthermore, it offers some deobfuscation techniques and decoding of other resources that were packed within the application.

2.4.9 Frida[8]

Frida is a dynamic code instrumentation toolkit. It supports various platforms (e.g., iOS, Android, Windows, etc.) and can be used to inject own code snippets into native apps that are running on the system. Therefore, it is a powerful tool for dynamic analysis that offers hooking into specific functions or changing a third-party program's behavior (e.g., bypass certificate pinning on Android).

2.4.10 Burp Suite[9]

Burp Suite is a hands-on tool that is used for security testing and analysis of web communication. It acts as a proxy between a client application and a web server and therefore allows inspecting or manipulating live data traffic.

[7] https://github.com/skylot/jadx
[8] https://frida.re/
[9] https://portswigger.net/burp

CHAPTER 3

Related Work

While there is a broad range of tools that are tailored to measure general network metrics (e.g., overall bandwidth or latency), net neutrality measurements are less common and usually aim to detect differentiation in terms of

- rate limiting (traffic shaping, traffic policing),
- traffic blocking (censorship),
- traffic manipulation,
- economic differentiation (differential pricing, zero-rating).

Rate limiting. Some early publications on the topic of network measurements present traffic shaping detection tools like *Glasnost* [9] or *NetPolice* [10]. Those tools were focused on detecting bandwidth throttling of specific protocols, with peer-to-peer file sharing protocols like BitTorrent leading the way of being discriminated against by many providers. *BonaFide* [11] and *MITATE* [12] were among the first tools that were specifically designed for net neutrality measurements within mobile networks. Unlike *Glasnost*, which was only available as Java applet and unfortunately consumed a lot of traffic to test for differentiation, those tools were implemented as smartphone applications and tried to minimize the amount of traffic that is needed to execute a test. Furthermore, they also considered additional factors that only exist in the cellular field (e.g., signal strength or location) to make the results more reliable. To adapt to the current times and better fit typical network utilization of cellular connections (peer-to-peer file sharing is mostly done on fixed-line connections), more recent tools started to focus on video streaming and VOIP protocols. Although these tools were designed to be extensible, it was necessary to manually provide specific implementation details for new protocols.

Instead of emulating protocols, Kakhki et al. [13] used a record-and-replay approach where pre-recorded application-generated traffic is used. This lowers the needed effort when adding new protocols or applications and allows to test closed source applications by treating them as a black box and just replaying its traffic. The most recent smartphone application that aims to detect traffic shaping and also uses this record-replay approach is *Wehe* [14, 15]. Addressing the issue of user impact and changing environmental circumstances, statistical methods are used to make the measurement results more reliable. More than 2 million measurements around the globe have been conducted, and anonymized measurement results are regularly published. Using their collected data, they identified 30 ISPs that throttle traffic to lower speeds based on the application being used. Regarding passive measurements, Flach et al. [16] got access to Google's CDN servers to investigate traffic policing for YouTube videos that had an impact on the video playback quality.

Traffic blocking and manipulation. The *Open Observatory of Network Interference* (*OONI*) [17, 18] is a versatile tool to detect traffic manipulation and censorship on a global scale. It is available as mobile and desktop application, and over 450 million measurements were openly published and can be browsed on their website. Often, the DNS protocol is leveraged to enforce nationwide censorship by blocking or hijacking queries [19]. Furthermore, providers have been caught hijacking unsuccessful DNS queries and falsely returning monetized results [20, 21] or even hijacking HTTP streams to deliver ads and malicious content [22] to their customers. While *OONI* is rather focused on detecting censorship, *RIPE Atlas* [23, 24] is a more flexible measurement platform that can not only be used to detect censorship [25], but also to investigate network routing information [26] or to conduct various protocol measurements [27]. However, *RIPE Atlas* does not offer mobile app-based measurements and is based on measurement probes that were distributed across the globe.

Economic differentiation and free riding. Differential pricing practices like zero-rating application-specific traffic were rarely seen in the fixed-line landscape but have become common over the past years in the cellular field. Although there are case studies that try to identify classification metrics used for economical differentiation [28] or investigate a concrete zero-rating offer by T-Mobile that targeted video streaming [29] there is no work that compares current zero-rating practices across different providers or countries. While those studies show that zero-rating can often be abused to get free data traffic, free-riding attacks have been a research topic in the mobile field even before zero-rating offers existed (e.g., by spurious TCP retransmission [30] or by abusing insecurities in VoLTE [31]).

Roaming. Due to the complex ecosystem that drives up cost and coordination effort, most studies that investigate roaming only involve a very limited amount of providers and countries. However, there is one large-scale study that utilized the *MONROE* [32, 33] measurement platform to analyze some general implications of

international data roaming [6]. The *MONROE* platform consists of sophisticated hardware probes that are currently deployed within four European countries (Norway, Sweden, Italy, and Spain). Each measurement probe has at least three modems, and SIM cards are provisioned by manually plugging them into the corresponding modems (usually orchestrated via email). The project has been open-sourced, and the access fees to use the current deployment for regular measurements start at 2,500 EUR for up to six months of usage. To the best of our knowledge, no current study investigates the effect that data roaming has on a provider's traffic differentiation mechanisms.

To summarize, two different practices can be observed for active net neutrality measurements in the mobile field. First, there are crowd-based measurement solutions, where the measurement tool is installed on a volunteer's smartphone (e.g., *Wehe*). While this approach lowers the economic effort that is needed for the test setup and usually makes it easier to increase the coverage and get a large amount of test units and results, it also has some drawbacks. Unwanted background activity, such as location changes by the user or data traffic caused by other apps, may occur during measurements, which might decrease the accuracy of technical experiments. Also, the data traffic that is caused during measurements should be kept at a minimum since the volunteered user is liable for any data charges (that quickly become excessively high when being abroad). Furthermore, because the telephone contract associated with the phone's SIM card is not exclusively used by the measurement unit and insight to the billed units is reserved to the contract owner, this approach is not suited to identify economic differentiation. Secondly, measurements can be performed on dedicated test units that are deployed and fully controlled by the test operator (e.g., *MONROE*). This usually implies higher setup costs but leads to more accurate measurement results. Besides active measurements, another approach is to leverage packet traces that were passively collected from a vantage point close to the destination of the data packets. Obviously, such studies can only be done when cooperating with a third party (e.g., a content provider) that processes a significant amount of data packets.

We observe that there is already a variety of measurement solutions that focus on the cellular field. *Wehe* and *OONI* have proven to be popular and effective tools to detect differentiation in terms of rate limiting and censorship. While these crowd-based solutions provide many results for common usage scenarios, they are only as good as their usage share and therefore may not detect violations, in particular, situations (e.g., users tend to measure differentiation in their home country but try not to "waste" any expensive data traffic when connected via roaming). Furthermore, they lack support to detect differential pricing practices because they have no insights into the units that were actually billed by the provider during a measurement. Although the *MONROE* measurement platform addresses some of these issues (e.g., supports detection of differential pricing mechanisms, test environment fully controlled by the test operator), it is simply not flexible enough to offer extensive roaming measurements in a well-scalable manner. Traditionally, SIM card and modem are physically colocated, and SIM cards need to be manually plugged

and removed in-between measurements. We identified the provisioning process as a major factor that drives up cost and coordination effort. Therefore, the MobileAtlas measurement platform decouples the physical SIM card from the location where the SIM card is actually used for a measurement, which fundamentally improves the scalability of large-scale roaming measurements. Furthermore, MobileAtlas provides a controlled environment, with no background noise of other apps, making it a powerful tool to detect fine-grained differentiation and differential pricing techniques. Besides data connections, MobileAtlas also allows the utilization of other mobile network capabilities (e.g., calls, SMS, and USSD) to conduct measurements. MobileAtlas aims to provide an open measurement platform that is easily extensible and therefore achieves maximum flexibility at minimal cost. Furthermore, this study is the first work that analyses zero-rating practices across multiple countries and investigates the effect that data roaming has on a provider's traffic differentiation mechanisms.

CHAPTER 4

Methodology

Measuring traffic differentiation at European MNOs involves a couple of factors and dimensions that need to be identified and structured to allow a scientific approach to the topic.

Our methodology allows analyzing

- different SIM cards (from different providers in different countries),
- that are provisioned with different zero-rating tariffs and applications,
- that are based on different Internet protocols (e.g., HTTP, HTTPS),
- within different countries (roaming measurements),
- to identify the used classifier metrics (e.g., IP- or SNI-based),
- to find differences and expose questionable practices in billing.

There are two parts to our methodology: analyzing the European market to acquire a set of SIM cards with zero-rating tariffs and characterizing the traffic differentiation mechanisms that are deployed within those SIM cards. The first step required us to do a market analysis that was used to choose a reasonable subset of SIM cards. For characterizing the traffic classifiers, we developed the MobileAtlas measurement platform to deploy the SIM cards to various countries and do controlled experiments that allow us to draw conclusions about the present traffic classification metrics.

4.1 EU-wide Market Analysis

To bring some structure to the chaos and find out which countries and providers are of particular interest, we started with an EU-wide market analysis. It has become increasingly popular that MNOs lease their wireless network infrastructure to Mobile Network Virtual Operators (MNVOs) that offer services to their customers but do not own any infrastructure. Compared to an MNO, becoming an MVNO is relatively easy and requires less financial effort. Thereby, many countries have got a vast amount of operators (e.g., Austria currently has about 40 MVNOs, despite being a relatively small country). However, due to well-established MNOs and the high fluctuation of MVNOs, the latter usually play a minor role in terms of actual market penetration. To limit the effort but accordingly respect the market situation, we limited our market analysis to bare-metal MNOs in every country. Furthermore, we neglected corporate IoT providers and focused on actual consumer-grade operators. After identifying the relevant players, we took a look at the available tariffs to find out whether they offer differential pricing or zero-rating programs. For this step, our primary source of information was a provider's website. The language barrier at foreign countries and complex tariff structures (e.g., prepaid vs. postpaid, minimum contract duration, additional packages that are only available in certain tariffs, etc.) made it somewhat cumbersome to get the required information. The results of our market analysis can be found in Section 5.1.

4.1.1 Acquiring SIM cards

The market analysis in the previous section provides a good overview of current operators and tariffs. Therefore, it was used to decide which SIM cards should be acquired be for our measurements. However, another factor that narrowed down the number of suitable countries was the current deployment of our MobileAtlas measurement platform that was utilized to take the measurements. Considering that we wanted to be able to compare differentiation between a domestic and roaming usage scenario, we were limited to those countries that MobileAtlas is currently deployed to (see Section 4.2.5). Since buying SIM cards from a remote country is usually not easily possible, and we were limited to tight funding and time constraints, we favored countries that are close to Austria and also do not require SIM card registration. An overview of the providers and tariffs that were finally acquired for our measurements can be found in Section 5.2.

4.2 MobileAtlas Measurement Platform

In this section, we present the MobileAtlas measurement platform we developed and used for our roaming measurements.

4.2.1 Components and Capabilities

As Figure 4.1 shows, the framework can be structured into three main components: SIM providers that allow sharing SIM card access, measurement probes that act as a local

breakout to the cellular network, and a management server that connects the prior two components and acts as command and control unit for the measurement probes.

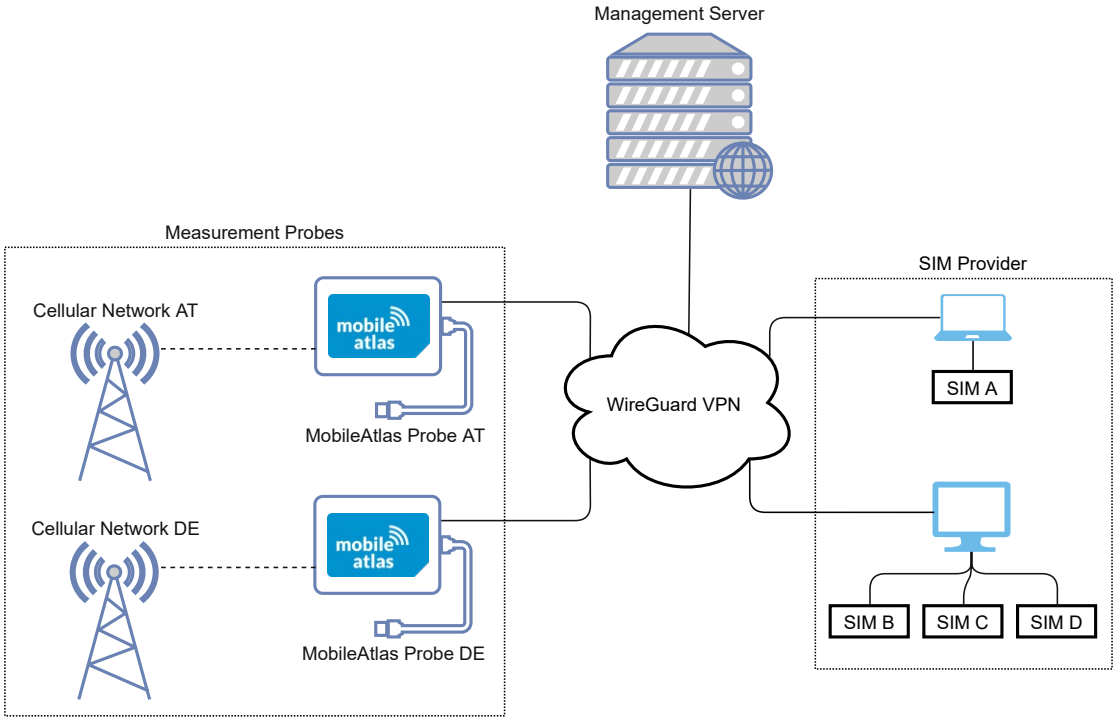


Figure 4.1: Architecture and components of the MobileAtlas measurement framework

SIM Provider

The SIM provider is used to remotely make one or more SIM cards available to the measurement platform. The program is written in Python 3 and runs on various operating systems (e.g., Linux, Windows). For communication between the computer and the SIM card, we rely on a modified version of pySim. Therefore, the user can choose between several options (e.g., PC/SC reader, Serial-based SIM card reader, Bluetooth rSAP, etc.) to connect the SIM card to the system (see Figure 4.2). When started, the program checks for SIM cards that are currently connected and queries the information that is required to uniquely identify the card (e.g., IMSI, ICCID). When the system is connected to the management server, those cards become available to the measurement platform and then can be virtually provisioned to any measurement probe.

Measurement Probe

MobileAtlas probes are responsible for measurement execution. Each probe consists of a single-board computer with at least an Internet uplink, USB host support, and a General-Purpose Input/Output (GPIO) interface. We chose the Raspberry Pi 4B as a

Figure 4.2: Various SIM reader devices that are supported by our SIM provider: a PC/SC reader and two different types of Serial-based SIM card reader

cost-effective platform with more than sufficient computing power for our tasks. For cellular connectivity, we use an LTE CAT 6 modem (Quectel EG25-G) that is connected to the Raspberry Pi with an (mPCIe to USB) LTE base HAT. To enable SIM tunnelling, the RST and I/O pin of the SIM slot on the LTE HAT are connected with the GPIO ports on the Raspberry Pi. For user-friendly deployment, we packaged the probe with all modules and antennas into a single case with just two connectors: an RJ45 Ethernet and a power connector (see Figure 4.3). A more detailed breakdown of all used hardware components can be found in the appendix.

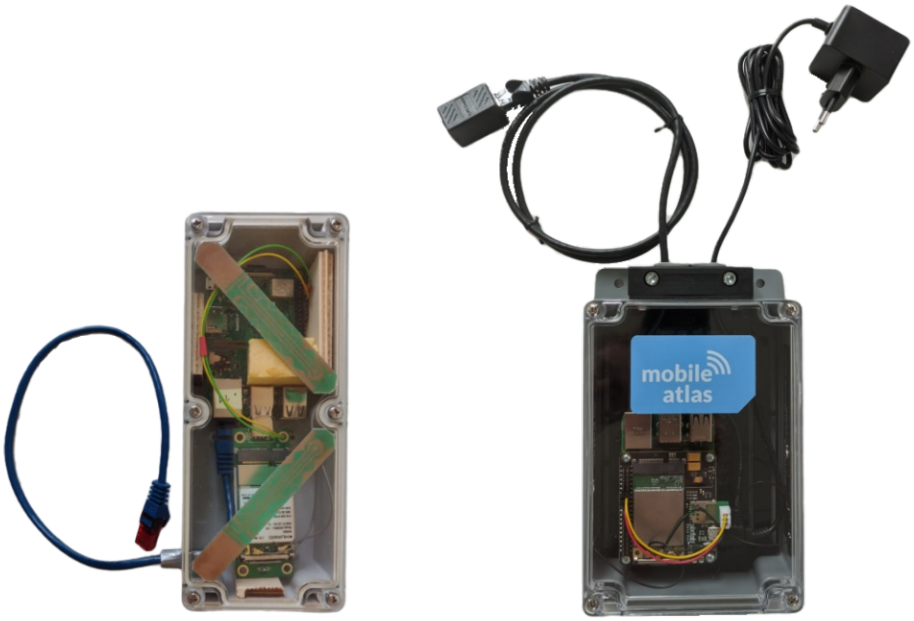


Figure 4.3: Measurement probe: first prototype (left) and official version (right)

The probe uses Raspberry Pi OS Lite (Debian-based) as operating system. For initial

deployment of the MobileAtlas software and to remotely change configurations or install additional software packages, we use Ansible. Most probe-specific software is written in Python 3. When the probe is powered on, it uses the Ethernet uplink to connect to our WireGuard VPN server. Within our VPN, the probe can be accessed without requiring a public IP address or any forwarded ports. To make the life of network administrators easier, the VPN is set as default gateway, which means the probe will only communicate via our server and does not cause any incoming or outgoing connections to other IP addresses. Currently, measurements are started manually via ssh, although we plan to integrate automated measurement execution and experiment scheduling into the management server in the near future. When a measurement is started on the probe, the requested SIM card is provisioned to the modem using our SIM tunneling technique. During measurements, various capabilities of the modem (e.g., starting a data connection, sending SMS or USSD messages, starting calls, sending custom AT-commands, etc.) can be used.

Management Server

The management server acts as WireGuard server and therefore enables communication between the SIM provider and measurement probe. Furthermore, it offers various REST endpoints that probes use to manage and update WireGuard keys or to send some basic system information (e.g., uptime, network status, CPU temperature, etc.) to the server on a regular basis. It also provides a useful web dashboard that gives an overview of deployed probes and allows sending commands to specific probes.

Mobile Atlas Dashboard

Probes Overview | Wireguard

Probes

Name	MAC	Last Service Startup	Polling Active	Status	Token Active	Git Commit
Germany	dc:a6:32:	2021-08-14 15:15:23	✓	online 2 days	✓	20685f8
Austria	dc:a6:32:	2021-08-14 15:48:33	✓	online 2 days	✓	489d9ca
Romania	dc:a6:32:	2021-08-14 15:15:36	✓	online 2 days	✓	5f58bac
Belgium	dc:a6:32:	2021-08-14 15:15:49	✓	online 2 days	✓	20685f8
Lost (Slovenia)	dc:a6:32:					
Croatia	dc:a6:32:	2021-08-14 15:15:25	✓	online 2 days	✓	a14d053
Finland	dc:a6:32:	2021-08-15 23:29:57	✓	online 22:37:57	✓	a14d053
Slovakia	dc:a6:32:	2021-08-14 15:15:36	✓	online 2 days	✓	a14d053
Slovenia	dc:a6:32:	2021-08-16 06:43:53	✓	online 15:23:58	✓	4f146f5

Figure 4.4: The MobileAtlas dashboard on the management server provides an overview of all probes that are currently deployed

4.2.2 SIM Tunneling

As already mentioned in Section 2.1, the communication between SIM card and modem is standardized by the ISO-7816 T=0 link protocol, as well as the ISO 7816-4 APDU application protocol. The protocol is byte-oriented, and timing constraints are not very strict, which makes it easy to relay (e.g., over TCP).

However, the SIM card receives a clock signal from the modem that is used as a baseline for sending bytes between SIM card and modem. Although the protocol specification allows varying clock speeds (e.g., slow down during idle time), usual modems just provide a fixed clock frequency and do not change it during operation.

We use the Raspberry Pi's Universal Asynchronous Receiver Transmitter (UART) interface in combination with a simple adapter circuitry (see Figure 4.5), to emulate the SIM card to the modem. Although a Universal Synchronous Asynchronous Receiver Transmitter (USART) interface would be even more suited for SIM card emulation, because it could directly use the modem's clock signal to synchronize transmission, there is also a way to use the more common UART interface when knowing the clock frequency that the modem provides to the SIM card. Therefore, we've measured the modem's clock frequency with an oscilloscope and configure the baudrate of our UART interface accordingly.

Furthermore, we've connected another GPIO port to the RST pin of the modem to reliably detect when the modem is resetting the SIM card. When a reset is detected, we send an Answer To Reset (ATR) to initiate communication with the modem.

Because our SIM tunnel implementation is aware of the initial setup process, the connection configuration on the two endpoints of the tunnel can be negotiated independently (e.g., connection speed at the SIM emulation is not dependent on the actual SIM card properties). Therefore, we've implemented support for multiple speed rates that can be offered by sending different ATR messages. Usually, the modem responds to an ATR message with a Protocol and Parameter Selection (PPS), where the fastest speed rate that is offered is selected.

Because modems normally support different operating voltages for SIM cards (1.8V, 3V, and 5V), we ignore the first reset that corresponds to 1.8V and just answer to the second one that corresponds to 3V and is within the tolerance of our UART voltage (3.3V).

After a successful connection setup, we just relay all APDUs that are received from the modem to our SIM provider. For expensive commands or long-lasting round-trip times, we can repeatedly signal Waiting Time eXtensions (WTX) to the modem.

4.2.3 Credit Checking

For tests on differential pricing, we need to know whether specific data traffic is deducted from the available credit units or funds. Because we want to minimize the required manual intervention and automate the test execution, we need to be able to automatically

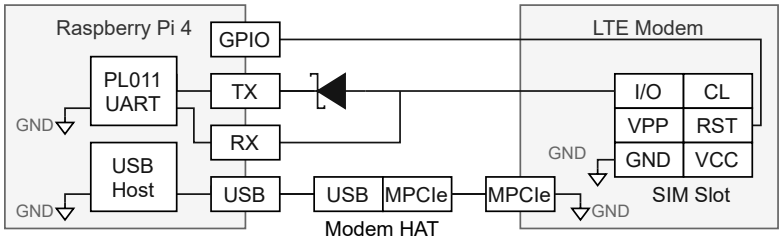


Figure 4.5: Minimalistic SIM interface

query a customer's credit information. Sadly, there is no standardized interface that allows retrieving the available credit information across different operators. However, most providers implement credit retrieval through one or more of the following ways:

SMS Message. Many providers allow requesting the available credit or consumed units via SMS (Short Message Service) message. To initiate retrieval, the customer has to send an SMS message with specific content to a specific number that is controlled by the provider. When the request is successfully submitted, the customer usually receives a response SMS message that contains the required information. Often, customers can make different requests (e.g., to another number or by sending different message content) to indicate what information they want to retrieve. For example, a provider might offer to query the overall funds of the account by sending a message to one number but also retrieving the used credit units of a particular tariff package by sending a message to another number.

USSD Code. USSD (Unstructured Supplementary Service Data) is a request-response-based communication protocol. The request is sent by the customer, who then receives the response from the network operator. Unlike SMS, where communication happens in an asynchronous manner, USSD operates within a real-time communication session. The session can provide contextual information, which allows the customer to navigate within complex menu structures that are offered by the network provider. While often credit information can be directly retrieved via USSD, it is sometimes used in conjunction with SMS. The customer makes a USSD request that is just is answered with an acknowledgment, and the actual response information is later on retrieved via SMS message.

Voice Call. Some operators provide service numbers that can be called to retrieve the current credit information. Often, it is required that the customer navigates through the voice menu before an actual request is issued. While again, this method is frequently used in conjunction with SMS (issuing the request via voice call, retrieving the information via SMS), some providers directly respond using the voice calls audio channel and a computer-generated voice speaking the output.

Website (Customer Area). Providers usually offer some kind of customer area or self-service that can be used to display the current credit information. When accessing

the web portal via the mobile data connection of the SIM card, the customer is often automatically recognized by its IP address. Besides automatic login, many providers offer a customer registration (e.g., using email/password) where various SIM cards that are owned by them can be connected to their account. Furthermore, some providers require the customer to receive a TAN SMS message at their phone number in order to prove ownership and complete the login process. After login, the customer can usually change tariff options, recharge their account, examine various account details and also access the used credit units or available funds. Compared to the previous methods, this way usually provides the most detailed and verbose information. Sometimes, a customer can even retrieve a connection-wise overview of the billed traffic.

Mobile App. Similar to the method that was described above, most providers offer a mobile app that can be used to access various customer and tariff-related information. Sometimes, the app just implements a web view of the customer area that is also accessible using the website. However, in many cases, we examined that the mobile app was retrieving the required information via a web API that provided even more detailed insights compared to the previous method. While the credit information on the website is often embedded in the HTML DOM tree, the web APIs usually provide structured JSON objects.

While a provider's website and the mobile app are easy to find, locating the available numbers for SMS, USSD, or voice-based credit retrieval is sometimes not that easy. Often they are not publicly announced on the provider's website but communicated through word-of-mouth in forums or on blog posts of knowledgeable customers. Furthermore, sometimes providers inform their customers how to retrieve the used units of a tariff package when it is activated by the customer.

Moreover, we identified several factors that influence credit checking and deviate between different operators and often even at different retrieval methods within one and the same operator:

Update Frequency, Update Latency. Often, providers don't update billing records in real-time but as a low priority task in the background with latency between minutes and half a day. Also, some views might be cached internally to minimize the stressed resources that are required when refreshing the view. Although some operators provide a timestamp that quotes the time when the credit information was updated, we noticed that in most cases, the quoted timestamp could not be trusted, and traffic is still billed retrospectively.

Unit Granularity (Displayed). In many cases, the credit units are only displayed in a very coarse resolution (e.g., "1.2 GB", so the smallest visible unit of granularity is 100 MB). We also experienced cases where the used resolution was dependent on the stated traffic size (e.g., using MB granularity when the traffic is less than 800 MB but switching to GB when it is above).

Unit Granularity (Internal/Billed). Similar to voice connections, operators usually bill the data traffic that was used by a customer in a session-based manner. Furthermore, providers usually round the bytes that were consumed within a session (i.e., a mobile data connection) to a certain amount of bytes.

Minimum Billing Unit. Again, this paradigm comes from the telephony world, where it was used at voice connections to generously round the used time units in favor of the operator. When the customer terminates a data connection where just a few bytes were transmitted, the operator rounds the used units up to the minimum billing unit (e.g., 1MB). This can cause an inflation of the billed units when a user has bad reception, resulting in many (interrupted) data connections with a very low amount of transmitted bytes.

Note that minimum billing unit and internal unit granularity correspond to incremental billing practices at voice connections. A 60/30 billing for a voice call resulted in a minimum of 60 seconds that were billed for a voice call and to a granularity of 30 seconds for calls that were longer than 60 seconds.

While the minimum billing unit and the internal unit granularity is the same for all retrieval methods, we noticed that update frequency and displayed unit granularity changes within different methods at the same provider. Furthermore, we observed that minimum billing unit and internal unit granularity could differ between domestic or roaming usage. Surprisingly, certain providers use more precise values when billing connections that were consumed in a roaming context and therefore billed by an external provider. Also, when concurrently using different retrieval methods within one and the same operator, results can differ because providers might use different update frequencies or caching strategies at different retrieval methods. Last but not least, querying the available credit using cellular functionalities (e.g., SMS message, voice call, or data connection) can cost credit itself and therefore have side effects on the billed credit units. This has to be considered when using automated credit checking to detect differential pricing.

CreditChecker Implementation

During our measurements, we had to implement the CreditChecker interface (cf. *CreditChecker* in Section 4.2.4) for every provider that was tested. We chose a mobile-app approach for almost all providers because it provides the most detailed billing information. Some operators even provide a connection-based enumeration of the billed data units. While SMS- or USSD-based credit retrieval is pretty straightforward, the app-based approach is much more cumbersome to implement. We had to reverse engineer the provider's mobile apps to find the appropriate API endpoints that are used to retrieve the credit from the network. We usually started off with the static analysis of the corresponding Android app. Thus, we decompiled the android app with JADX, to obtain a human-readable representation of the program. Because nowadays, nearly all apps

are heavily obfuscated, we continued with dynamic analysis of the app. We installed the relevant app on a rooted Nexus 4 device and used Frida to hook into the target process. At apps that allowed to bypass certificate pinning, we used Burp to intercept the communication between the app and the provider's web server. Thereby, we obtained the relevant REST endpoints for login and credit retrieval. However, some apps had more sophisticated measures against bypassing certificate pinning. Our second approach usually was to use Frida to directly hook into the HTTP-library calls (e.g., OkHttp, HttpClient) that were used by the app to craft the actual HTTP requests. As before, this allowed us to eavesdrop on the REST communication and to identify the relevant endpoints. Moreover, in some cases, it was useful to inspect or execute outdated versions of the mobile app because those implement weaker security measures than the most current version.

4.2.4 Software Architecture

All main software components have been implemented in Python 3 for rapid prototyping. While the software architecture of the SIM provider and the management server are rather simple, the measurement probe is not only the most crucial but also the most complex component of the framework.

Probe Startup Services

The MobileAtlas probe software provides two systemd-services that communicate with the management server: The *wireguard-register* service takes care of the WireGuard configuration. It receives the basic configuration at first startup and updates its keys to the server when necessary. The *mobile-atlas* service is responsible for the actual command and control communication with the management server. It notifies the server after every reboot and regularly uploads basic system information. Furthermore, it supports processing custom commands (e.g., to pull framework updates from a git repository) that are received from the server. Communication with all REST interfaces of the management server is secured using token-based authentication. Prior to obtaining a valid token, the MAC address of the corresponding probe needs to be activated on the management server.

Additionally, two native systemd-services are activated during the installation of the framework: Since the WireGuard service that was mentioned above just takes care of key configuration, a second WireGuard service is used to actually connect the VPN interface. The *wg-quick* activates the WireGuard VPN and also installs the interface as default gateway. Furthermore, we use the *watchdog* service to ensure continuous availability of our measurement probes. Besides a hardware watchdog that kicks in when the system hangs in a non-responsive state, there is also a software watchdog that reboots in case the management server is not reachable via the VPN connection.

Measurement Execution

When a new measurement is executed on the probe, it reads the test configuration (can be specified via JSON file and via command-line arguments), and when successfully parsed, power-cycles the attached modem device. Furthermore, it connects to a specific SIM provider and requests the appropriate SIM card by its IMSI. The SIM provider accepts it and bidirectionally forwards APDU traffic. On the probe's side, a new network namespace is created to fully isolate the measurement from the host system. Within the measurement namespace, a new ModemManager and NetworkManager instance is launched to handle the initialization of the modem connection, as well as the initialization of the networking environment. Because some experiments might require Internet connectivity within the measurement namespace (without using the modems data connection), the framework also implements a virtual Ethernet bridge between the host and measurement namespace that can be turned off and on (i.e., configured as default gateway), respectively. When using the framework's debugging functionality, the virtual Ethernet bridge is also required because the remote debugging connection is port-forwarded from the host to the measurement namespace. Next, the experiment functionality is executed within the namespace and its adopted network stack. During the experiment, a tcpdump instance records the whole traffic for optional analysis. Any direct test case results will be stored in a JSON file. To increase traceability of our measurements, we also store the full debug logs of ModemManager and NetworkManager and a complete dump of all APDUs that were transmitted between modem and SIM card. Finally, all test artifacts will be stored in a temporary output directory. In the following, we'd like to introduce the most relevant software components that are used when a measurement is conducted.

Mediator. This module provides an interface that allows sending control messages to the modem and to the measurement namespace's network stack. It uses the D-Bus (via GObject-Introspection) to directly interact with ModemManager and NetworkManager. Thereby, it also receives asynchronous notifications when the state of the modem or network is changed. Other components can not only directly call the mediators functionality (e.g., connecting the modem or sending an SMS), but also subscribe to relevant events (e.g., changed connection-state, SMS received) and will get notified upon.

Tests and Payloads. Actions that should be executed during an experiment are expressed as payloads and tests. A test usually is composed of one or more payloads that are processed sequentially. Both test and payload can interact with the mediator object and have to predefine the capabilities (e.g., send SMS or USSD codes, make calls, etc.) that are required for successful execution. When a test or payload requests a specific capability, the mediator object will automatically send out notifications accordingly to the requested event type. A test usually corresponds to a specific experiment and parses its parameters dynamically from the test configuration that is provided when executing the measurement. Payloads are usually designed to be reusable within different tests and therefore define

the required parameters within its constructor. Furthermore, tests and payloads heavily rely on inheritance to strengthen cohesion and prevent duplicated code (see Figure 4.6).

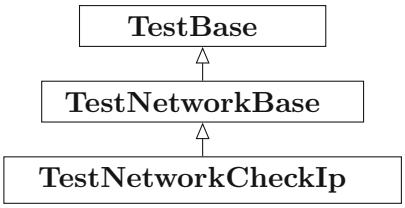


Figure 4.6: *TestNetworkBase* inherits from *TestBase* and implements all network related functionalities (e.g., starting/stopping a data connection using the right apn) that are required by *TestNetworkCheckIp*

CreditChecker. Every test has to define whether it is a billing test that requires to record and monitor the credit that was consumed during the experiment. Similar to tests and payloads, a credit checker attaches to the mediator and predefines the required capabilities. Obviously, every provider offers different ways in which customers can retrieve the consumed or available credit units. Because MobileAtlas can use all functionalities of the attached modem, it basically supports all methods for credit checking that were mentioned in Section 4.2.3. However, a specific CreditChecker has to be manually implemented for every provider (and sometimes even different ones for specific tariffs). To make the consumed credit comparable, we define a collective interface that lists the most commonly available used units:

- **credit_consumed_credit:** a decimal value that represents the actual monetary value that was deducted from the available credit
- **traffic_bytes_upstream:** the amount of transmitted bytes that was billed
- **traffic_bytes_downstream:** the amount of received bytes that was billed
- **traffic_bytes_total:** the total amount of bytes that was billed
- **traffic_cnt_connections:** the amount of data connections that were recognized by billing
- **timestamp_effective_date:** a timestamp that points to the moment when billing was updated the last time
- **bill_dump:** more verbose information that was retrieved from the operator (e.g., JSON that contains the full response from the provider's API endpoint)

When executing a billing measurement, the responsible test class communicates the units that were caused during the test to the CreditChecker. Furthermore, the test class takes care of retrieving the base bill that will be used as a reference point before the actual test payload is executed (cf. Figure 4.7). After the actual

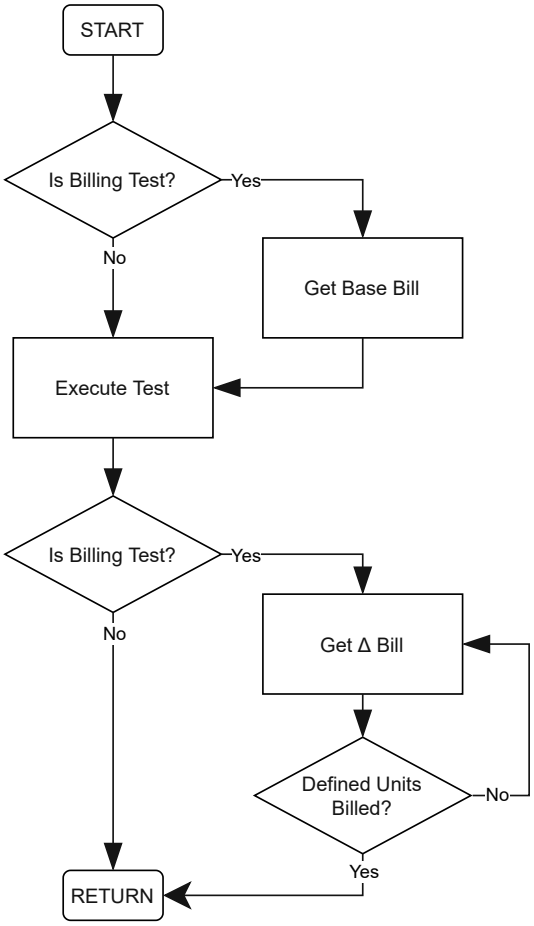


Figure 4.7: The CreditChecker retrieves the bill before and after the payload is executed

test payload is processed, the CreditChecker becomes active again and periodically checks for newly billed credit units. When the signaled units are recognized (or when an available timestamp corresponds to a mature effective billing date), the experiment is finished and will gracefully terminate. Because the CreditChecker has to state the modem functionality that is required to query the credit information, the test class will put the modem into airplane mode when no modem functionality is needed (e.g., when the provider's website is used with email/password-based login). This is because some providers will bill the consumed units more quickly when the modem fully terminates the connection to the cellular network.

4.2.5 Current Deployment

We mainly used our personal network of friends and family to find people that willingly support the MobileAtlas project by hosting a measurement probe. As shown in Figure 4.8, we currently (2021-09) deployed probes in eight European countries: Aus-

tria, Belgium, Croatia, Finland, Germany, Romania, Slovakia, and Slovenia. Because MobileAtlas is extensible, new hosts could easily extend the set of countries. The requirements to run a measurement probe are a free power outlet for the power supply, network access (with DHCP) via Ethernet, and mobile network coverage. We argue that for most experiments, one probe per country is sufficient because our test metrics probe network properties and not the properties of individual base stations.

Figure 4.8: Current (2021-09) coverage of MobileAtlas within Europe [34]

4.3 Experiment Implementation

For tests on differential pricing and, more specifically, zero-rating, we need to know whether specific traffic is deducted from the available credit units or funds. To cope with different update latency of consumed units and to enable running multiple payloads without in-between waiting for the billing records to update, we use binary exponents, i.e., every payload uses traffic amounts selected from $baseunit \times 2^{testid}$. For example, the first payload might use 1 MB, the second 2 MB, the third 4 MB, and the fourth 8

MB. When the final traffic billing arrives (which in our case is a control payload that is always billed), we can unambiguously deduct which payloads were counted towards the customer's bill.

To reveal potential metrics that are used for classification by a certain provider, we designed three different tests. Because most web services nowadays are built upon HTTPS communication, our tests focus on web resources as well. Thereby, basically any service that uses HTTPS communication can be tested by providing an appropriate web endpoint to the test script. Because we also want to take a peek into the past and into the future and many web servers offer multiple protocols to serve their content anyway, MobileAtlas implements support for HTTP, HTTPS, and HTTP3/QUIC.

To identify endpoints that might be of particular interest (i.e., endpoints that correspond to a zero-rated app), we usually collected a traffic dump of the target application.

TestNetworkZero

This test is responsible for validating that the provided web resource is actually zero-rated by the provider. Furthermore, the test configuration allows providing a list of protocols that are tested during the experiment. Per default *HTTPS*, *HTTP* and *HTTP3/QUIC* are used. As Algorithm 4.1 shows, the list of protocols is sequentially processed with increasing payload size. When executing the payload for a concrete protocol, the test repeatedly requests the resource using the corresponding protocol. For repeated requests, the payload implementation ensures that the DNS query is only issued once. Finally, the test generates control traffic to a third party that is not part of any zero-rating program and therefore normally billed. As previously described, the test terminates as soon as the control traffic is recognized. Figure 4.9 gives an overview of the involved actors and the traffic flow when the test is executed for an application with the hostname *application.com*.

Algorithm 4.1: Pseudocode of TestNetworkZero

```
1 TestNetworkZero (R, B, P)
      inputs: Web Resource R; Base Size B; Protocol List P = [https, http, quic]
2     size ← B;
3     foreach p_i ∈ P do
4         ExecutePayloadWeb(R, size, p_i);
5         size ← 2 × size;
6     end
7     ExecutePayloadCtrl(size);
8     return;
```

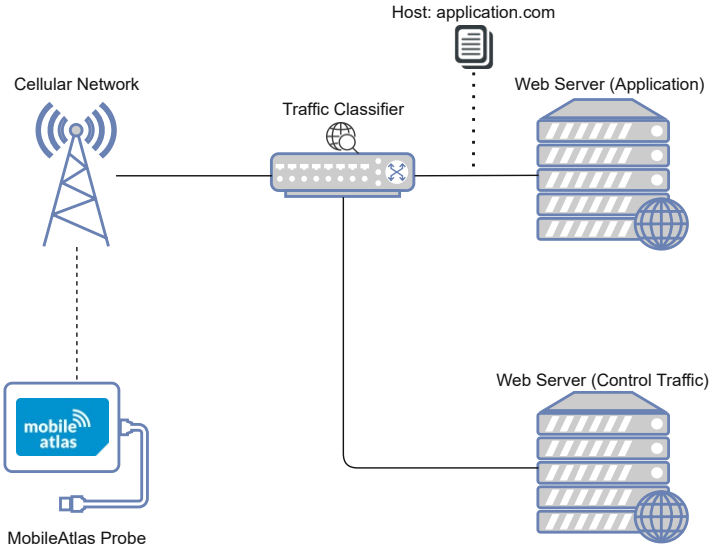


Figure 4.9: Involved actors and traffic flow of TestNetworkZero

TestNetworkZeroCheckSni

This test retrieves the IP address of the server that holds the provided web resource. It then automatically launches an EC2-instance and forwards the corresponding ports for the protocols that should be tested (e.g., TCP80 and TCP443 for HTTP and HTTPS and UDP443 for QUIC). Thus, when a TCP connection to the freshly spawned EC2 server is initiated on port 80, the connection is forwarded to the original web server. Thereby, the same content is served, although the data packet that is processed by the provider is headed to a different IP address. When executing the payload for a certain protocol, the measurement environment pins the hostname of the original web resource to the IP address of the EC2 instance, resulting in a spoofed IP address during DNS lookup. Therefore, the measurement is also conducted against a third-party IP address (i.e., against the EC2 server). Figure 4.10 gives an overview of the involved actors and the traffic flow during this test. When the data packets are passing the classifier, the hostname within the packets matches the one from the application. However, the IP address of the packets does not match the address of the application's web server because the packets are headed to the EC2 instance. Furthermore, the provider does not know about the port forwarding because this happens behind closed doors on the EC2 instance. However, the content of the data packets is equal to the previous test because the EC2 instance acts as a proxy to the actual application's web server.

TestNetworkZeroCheckIp

While no external server is needed for this test, the actual hostname that is sent within the target protocol is replaced. Again we get the required behavior by spoofing DNS

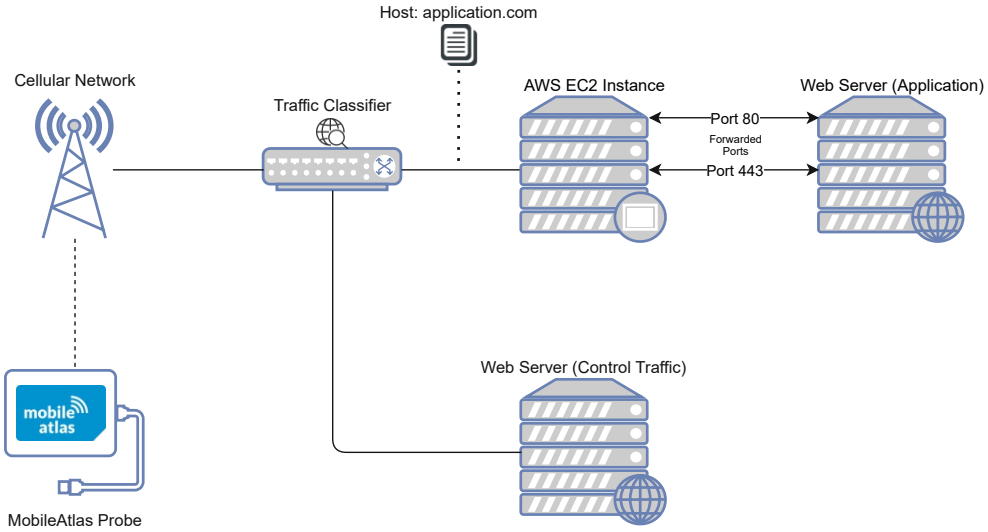


Figure 4.10: Involved actors and traffic flow of TestNetworkZeroCheckSni

responses. The hostname of the original web resource is replaced by *example.com*, and when requesting the IP address of the target resource, the original IP address is returned. Therefore, the program connects to the right IP address but sends a different hostname (e.g., for the Host-/SNI header) at the protocol layer. Figure 4.11 gives an overview of the involved actors and the traffic flow during this test. Although the packets are sent to the real application's web server, they do not contain the actual hostname because it was previously exchanged with a dummy value (*example.com*).

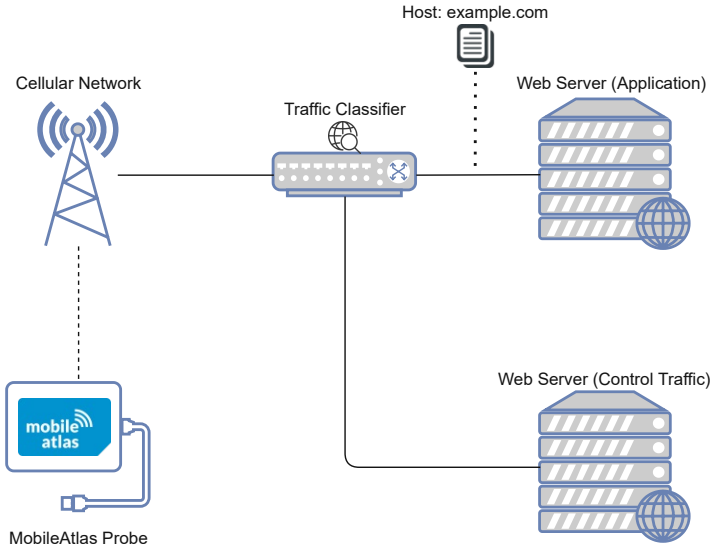


Figure 4.11: Involved actors and traffic flow of TestNetworkZeroCheckIp

4.3.1 Experiment Result Interpretation

We provide three imaginary example test results to showcase our methodology and giving an explanation on how to interpret specific characteristics. Because it was also the default value for most of our measurements, the base size that is used for the first payload is 1 MB. Thereby the particular payloads correspond to the following values: HTTPS ≙ 1 MB, HTTP ≙ 2 MB, QUIC ≙ 4 MB and Ctrl ≙ 8 MB.

Table 4.1 represents the results when the experiments are executed on a resource that is not part of any zero-rating program and therefore fully billed by the provider. Because the single payloads add up to 15 MB, this amounts to the final bill.

Test	Billed	HTTPS	HTTP	QUIC	Ctrl
TestNetworkZero	15 MB	●	●	●	●
TestNetworkZeroCheckSni	15 MB	●	●	●	●
TestNetworkZeroCheckIp	15 MB	●	●	●	●

● billed traffic ○ zero-rated traffic

Table 4.1: The traffic classifier did not zero-rate any traffic that was sent within the test

Table 4.2 represents the results when the provider relies on a hostname-based classification approach. The second line in the table suggests that the hostname can be used for free-riding, since the actual target IP address of the sent packets corresponds to a freshly spawned EC2 instance. Furthermore, the third line shows that packets to the actual application server are fully billed when they are sent with the wrong hostname.

Test	Billed	HTTPS	HTTP	QUIC	Ctrl
TestNetworkZero	8 MB	○	○	○	●
TestNetworkZeroCheckSni	8 MB	○	○	○	●
TestNetworkZeroCheckIp	15 MB	●	●	●	●

● billed traffic ○ zero-rated traffic

Table 4.2: The provider's classifier used DPI to inspect the hostname inside the packet (e.g., via Host- or SNI-Header)

Table 4.3 represents the results when the provider relies on an IP-based classification approach. No matter which hostname is sent, the server just decides based on the IP address inside the packet header.

Test	Billed	HTTPS	HTTP	QUIC	Ctrl
TestNetworkZero	8 MB	○	○	○	●
TestNetworkZeroCheckSni	15 MB	●	●	●	●
TestNetworkZeroCheckIp	8 MB	○	○	○	●

● billed traffic ○ zero-rated traffic

Table 4.3: The provider used an IP-based classification approach

Obviously, multiple different approaches can also be used in combination. For example, some providers deploy classification that uses hostnames, as well as IP addresses.

4.4 Ethical Considerations

Ethical considerations are crucial to the field of measurements, especially with measurements conducted in live production systems. While having diverse ethical considerations throughout our study, the following aspects are especially important:

Used SIM cards Since some measurements or the SIM tunneling technique could be viewed as illegitimate use by the operator, we only used SIM cards that were specifically purchased for this thesis and were registered to ourselves when SIM card registration was required. Thus, it would not affect any other user in a negative way, in case a SIM card gets blocked by the provider (although we did not experience any blocked SIM cards or terminated contracts).

Influencing the live system Because our measurements were conducted in real cellular networks, we took special care to ensure that no damage is caused. Although our SIM tunneling technique allows changing countries in an irregular and unnaturally fast way (i.e., within several seconds), we manually restrict the minimum duration between country switches to two hours. Furthermore, we ensured that our experiments mimic normal user behavior and do not stress any resources excessively (e.g., limiting the frequency of SMS-based credit checking to several minutes, using (undisclosed) provider APIs with caution, etc.). Although our experiments request a tested resource from a web server in a repeatedly and unnatural manner, we do not violate any protocol specification and argue that any web server is capable of serving the sequentially queried content without occurrence of any negative side effects.

Probe security Our measurement probes are deployed to foreign local networks and therefore need to be secured accordingly to not cause any inconvenience to our contributors. We ensure that the probe only communicates in an encrypted manner via our VPN server. To keep the environmental emissions (e.g., heat, RF signal,

etc.) as low as possible, we physically turn off the modem when the probe is in idle mode, and currently, no experiment is running.

CHAPTER 5

Results

5.1 EU-wide Market Analysis

As already mentioned in Section 4.1 we started with an EU-wide market analysis to get an overview of current providers and available tariffs. As Table 5.1 shows, SIM card registration is required in 14 of 27 EU countries (ca. 52%) [35]. Furthermore, according to our market analysis, 24 EU countries (ca. 89%) currently have implemented differential pricing or zero-rating offers. The table also shows whether MobileAtlas is currently deployed in the country since this was a fundamental requirement for the selection of the target countries for our measurements.

In the following sections, we present a country-wise overview of the results of the market analysis. Please note that the analysis was conducted in May 2021 on a best effort basis. As already mentioned in Section 4.1, the language barrier at foreign countries, chaotic provider websites, complex tariff structures, and short-lived offers make it hard to extract all relevant information. Furthermore, our goal was to provide a brief overview of the current market situation and identify (differential pricing) tariffs of interest. Therefore, we do not claim that the provided information is perfectly accurate or legally correct (as we often shorten provider names, etc.). Also, we use the word zero-rating in a broader meaning for both zero-rating (i.e., unlimited access to a specific resource) and differential pricing offers that only provider a limited quota (e.g., 10 GB) for the promoted application.

Country	SIM Registration	Diff. Pricing	Probe	NRA
Austria	●	●	●	RTR [36]
Belgium	●	●	●	BIPT [37]
Bulgaria	●	●	○	CRC [38]
Croatia	○	●	●	HAKOM [39]
Cyprus	●	○	○	OCECPR [40]
Czech Republic	○	●	○	CTU [41]
Denmark	○	●	○	DBA [42]
Estonia	○	●	○	ETRA [43]
Finland	○	○	●	FICORA [44]
France	●	●	○	ARCEP [45]
Germany	●	●	●	BNetzA [46]
Greece	●	●	○	EETT [47]
Hungary	●	●	○	NMHH [48]
Ireland	○	○	○	ComReg [49]
Italy	●	●	○	AGCOM [50]
Latvia	○	●	○	SPRK [51]
Lithuania	○	●	○	RRT [52]
Luxembourg	●	●	○	ILR [53]
Malta	●	●	○	MCA [54]
Netherlands	○	●	○	ACM [55]
Poland	●	●	○	UKE [56]
Portugal	○	●	○	ANACOM [57]
Romania	○	●	●	ANCOM [58]
Slovakia	●	●	●	RU [59]
Slovenia	○	●	●	AKOS [60]
Spain	●	●	○	CNMC [61]
Sweden	○	●	○	PTS [62]

● yes ○ no

Table 5.1: Overview of all analyzed countries

5.1.1 Austria

MCC/MNC*	Provider	Alternative Name	Market Share†	Zero-Rating Program
23201	A1 [63]	Telekom Austria	39.9%	A1 Free Stream [64]
23203	Magenta [65]	T-Mobile	25.3%	Magenta Stream [66]
23205	Drei [67]	Orange	23.6%	MyStream [68]

*According to RTR [69] †According to RTR Telekom Monitor Q2 2020 [70]

Table 5.2: MNOs in Austria

5.1.2 Belgium

MCC/MNC*	Provider	Alternative Name	Market Share*	Zero-Rating Program
20601	Proximus [71]	Belgacom	46.4%	Epic [72]
20610	Orange [73]	Mobistar	31.0%	—
20620	BASE [74]	Telenet	22.6%	—

*According to messaggio.com [75]

Table 5.3: MNOs in Belgium

Table 5.3 provides an overview of our market analysis results of Belgian providers. Although Orange had implemented so-called Fun Passes in 2019 (e.g., "Fun Pass Social Media" and "Fun Pass video"), those offers were discontinued on November 30th, 2019 [76]. While BASE does not directly offer any zero-rating programs, its parent company Telenet offers Free-G [77].

5.1.3 Bulgaria

MCC/MNC*	Provider	Alternative Name	Market Share†	Zero-Rating Program
28401	A1[78]	MTel, Mobiltel, Citron	38.0%	A1 One Traffic pass [79]
28405	Telenor [80]	Globul, Cosmo	32.0%	Postpaid Traffic pass [81]
28403	VIVAcom [82]	Vivatel	29.0%	—
28413	Ti.com‡ [83]	Max Telecom	<1%	—
28411	Bulsatcom‡ [84]		<1%	—

*According to messaggio.com [85] †According to alertify.eu [86] ‡Only available in restricted urban spaces, int. roaming is not supported

Table 5.4: MNOs in Bulgaria

5.1.4 Croatia

MCC/MNC*	Provider	Alternative Name	Market Share*	Zero-Rating Program
21901	Hrvatski Telekom [87]	T-Mobile, Simpa	46.3%	StreamOn [88]
21910	A1 [89]	vip	35.0%	NON STOP SOCIAL [90]
21902	telemach [91]	Tele2	18.8%	—

*According to messaggio.com [92]

Table 5.5: MNOs in Croatia

5.1.5 Cyprus

MCC/MNC*	Provider	Alternative Name	Market Share*	Zero-Rating Program
28010	epic [93]	MTN, Scancom	49.3%	—
28001	Cyta [94]	Mobistar	36.5%	—
28020	PrimeTel [95]	Telenet	14.2%	—

*According to messaggio.com [96]

Table 5.6: MNOs in Cyprus

As Table 5.6 shows, Cyprus is one of only three European countries where currently no zero-rating tariffs are offered by providers. However, before MNT was rebranded to epic (in 2019), it provided unlimited free access to Facebook via the Facebook Zero program [97].

5.1.6 Czech Republic

MCC/MNC*	Provider	Alternative Name	Market Share*	Zero-Rating Program
23001	T-Mobile [98]	Paegas	38.9%	—
23002	O2 [99]	Telefónica, Eurotel, Český Telecom	36.4%	—
23003	Vodafone [100]	Oskar	24.8%	Vodafone Pass [101]

*According to messaggio.com [102]

Table 5.7: MNOs in Czech Republic

Table 5.7 provides an overview of our market analysis results in the Czech Republic. An earlier zero-rating program called StreamOn at T-Mobile was discontinued in November 2019 because of meager user interest and adoption [103].

5.1.7 Denmark

MCC/MNC*	Provider	Alternative Name	Market Share*	Zero-Rating Program
23801	TDC [104]	youSee	40.9%	YouSee Music [105]
23802	Telenor† [106]	Sonofon, TT-Netvork	22.5%	—
23820	Telia† [107]		19.4%	—
23806	3 [108]	Tre	17.1%	—

*According to messaggio.com [109] †Telenor and Telia share parts of their network infrastructure

Table 5.8: MNOs in Denmark

5.1.8 Estonia

MCC/MNC*	Provider	Alternative Name	Market Share*	Zero-Rating Program
24801	Telia [110]	EMT	45.8%	Spotify [111]
24802	Elisa [112]	Radiolinja	27.6%	—
24803	Tele2 [113]	Q-GSM	26.6%	—

*According to messaggio.com [114]

Table 5.9: MNOs in Estonia

5.1.9 Finland

MCC/MNC*	Provider	Alternative Name	Market Share†	Zero-Rating Program
24405	Elisa [115]	Saunalahti, Radiolinja	35.0%	—
24491	Telia [116]	Telecom, Sonera	34.0%	—
24403	DNA [117]	—	22.0%	—
24414	Ålcom [118]	ÅMT	<9.0%	—

*According to FICORA [119] †According to Statista [120]

Table 5.10: MNOs in Finland

As Table 5.10 shows, Finland is one of only three European countries where currently no zero-rating tariffs are offered by providers. However, in early days of zero-rating offers Saunalahti (nowadays Elisa) took part in the Facebook Zero program that offered free unlimited access to Facebook [121].

5.1.10 France

MCC/MNC*	Provider	Alternative Name	Market Share*	Zero-Rating Program
20801	Orange [122]	Itineris	39.9%	—
20810	SFR [123]		24.1%	—
20820	Bouygues [124]		20.0%	B.tv [125]
20815	Free Mobile [126]	Iliad	16.0%	—

*According to messaggio.com [127]

Table 5.11: MNOs in France

5.1.11 Germany

MCC/MNC*	Provider	Alternative Name	Market Share†	Zero-Rating Program
26202	Vodafone [128]		38.13%	Vodafone Pass [129]
26201	Telekom [130]	T-Mobile	32.35%	Stream On [131]
26203	O2 [132]	Telefónica, E-Plus	29.52%	—

*According to messaggio.com [133] †According to BNetzA [134]

Table 5.12: MNOs in Germany

5.1.12 Greece

MCC/MNC*	Provider	Alternative Name	Market Share*	Zero-Rating Program
20201	Cosmote [135]		49.2%	Chat Now [136]
20205	Vodafone [137]	Panafon	30.3%	Vodafone Pass [138]
20210	Wind [139]	Telestet, TIM, Q-telecom	20.4%	—

*According to messaggio.com [140]

Table 5.13: MNOs in Greece

Table 5.13 provides an overview of our market analysis results of Greek providers. An earlier zero-rating tariff by Wind that included free WhatsApp traffic [141] is no longer available.

5.1.13 Hungary

MCC/MNC*	Provider	Alternative Name	Market Share*	Zero-Rating Program
21630	Telekom [142]	Westel, T-Mobile	44.2%	ZENE OPCIÓ [143, 144]
21601	Telenor [145]	Pannon	29.7%	HelloChat [146]
21670	Vodafone [147]	UPC Mobile	26.1%	Vodafone Pass [148]
21603	DIGIMobil [149]		<1%	—

*According to messaggio.com [150]

Table 5.14: MNOs in Hungary

Table 5.13 provides an overview of our market analysis results of Hungarian providers. Compared to other countries with SIM registration, where it is only necessary to prove the identity once, Hungarian SIM registration laws are very strict, and the identity of the customer has to be verified regularly on a yearly basis.

5.1.14 Ireland

MCC/MNC*	Provider	Alternative Name	Market Share*	Zero-Rating Program
27205	3 [151]	O2	43.0%	—
27201	Vodafone [152]	Eircell	37.4%	—
27203	eir [153]	Meteor, eMobile	19.6%	—

*According to messaggio.com [154]

Table 5.15: MNOs in Ireland

As Table 5.15 shows, there are currently no commercial zero-rating offers in Ireland. However, several providers introduced zero-rating for healthcare and educational resources to assist consumers during COVID-19 [155].

5.1.15 Italy

MCC/MNC*	Provider	Alternative Name	Market Share†	Zero-Rating Program
22201	TIM [156]	Telecom Italia	32.2%	GIGA ILLIMITATI[157]
22210	Vodafone [158]	Omnitel	30.8%	Vodafone Pass [159]
22299	WINDTRE [160]	WIND, Tre	29.2%	—
22250	Iliad [161]		2.8%	—

*According to messaggio.com [162] †According to Statista [163]

Table 5.16: MNOs in Italy

Table 5.16 provides an overview of our market analysis results of Italian providers. An earlier zero-rating tariff by Windtre was criticized by the corresponding NRA and later on discontinued [164], and several providers have offered free zero-rating for educational purposes during the COVID-19 crisis [165].

5.1.16 Latvia

MCC/MNC*	Provider	Alternative Name	Market Share*	Zero-Rating Program
24701	LMT [166]		41.6%	—
24702	Tele2 [167]		40.3%	—
24705	Bite [168]		18.1%	Neierobežots Internets Aplikācijām [169]

*According to messaggio.com [170]

Table 5.17: MNOs in Latvia

5.1.17 Lithuania

MCC/MNC*	Provider	Alternative Name	Market Share*	Zero-Rating Program
24603	Tele2 [171]		43.7%	—
24601	Telia [172]	Omnitel, Teo LT	35.5%	—
24602	Bite [173]		20.8%	Nemokamos paslaugos [174]

*According to messaggio.com [175]

Table 5.18: MNOs in Lithuania

Table 5.18 provides an overview of our market analysis results of Lithuanian providers. Although Tele2 does not directly implement any zero-rating tariffs, they own Pildyk [176], which is a prepaid sub-brand that offers zero-rating [177]. The same holds for Telia and it's prepaid sub-brand Ežys [178, 179].

5.1.18 Luxembourg

MCC/MNC*	Provider	Alternative Name	Market Share*	Zero-Rating Program
27077	Tango [180]		46.2%	Tango Infinity [181]
27001	POST [182]	LuxGSM, P&T	41.3%	Streaming & Social [183]
27099	Orange [184]	VOXmobile	12.5%	—
27005	Luxembourg Online [185]		<1%	—

*According to messaggio.com [186]

Table 5.19: MNOs in Luxembourg

5.1.19 Malta

MCC/MNC*	Provider	Alternative Name	Market Share*	Zero-Rating Program
27801	epic [187]	Vodafone, Telecell	49.3%	—
27821	GO [188]	Maltacom	38.1%	WildCard [189]
27877	Melita [190]		12.6%	—

*According to messaggio.com [191]

Table 5.20: MNOs in Malta

5.1.20 Netherlands

MCC/MNC*	Provider	Alternative Name	Market Share†	Zero-Rating Program
20408	KPN [192]	Telfort	27.5%	—
20416	T-Mobile [193]	Tele2, Orange	27.5%	Datavrije Muziek [194]
20404	Vodafone [195]	Libertel, VodafoneZiggo	22.5%	—

*According to messaggio.com [196] †According to ACM [197]

Table 5.21: MNOs in Netherlands

5.1.21 Poland

MCC/MNC*	Provider	Alternative Name	Market Share†	Zero-Rating Program
26006	Play [198]	P4	29.0%	PLAY NOW [199]
26003	Orange [200]	Idea	27.3%	Flex Pass [201]
26001	PLUS [202]	Polkomtel, Aero2	21.3%	Darmowytransfer [203]
26002	T-Mobile [202]	ERA	18.9%	Supernet Video [204]

*According to messaggio.com [205] †According to Statista [206]

Table 5.22: MNOs in Poland

5.1.22 Portugal

MCC/MNC*	Provider	Alternative Name	Market Share*	Zero-Rating Program
26806	MEO [207]	TMN	46.1%	Smart Net [208]
26801	Vodafone [209]	Telecel	28.4%	Vodafone Pass [210]
26803	NOS [211]	Optimus	25.5%	WTF [212]

*According to messaggio.com [213]

Table 5.23: MNOs in Portugal

5.1.23 Romania

MCC/MNC*	Provider	Alternative Name	Market Share†	Zero-Rating Program
22610	Orange [214]	Dialog	38.0%	Abonamente Fun [215]
22601	Vodafone [216]	Connex	30.0%	Vodafone Pass [217]
22603	Telekom [218]	Cosmote	15.0%	Oferta Promoţională Messaging [219]
22605	Digi [220]		13.0%	—

*According to messaggio.com [221] †According to Statista [222]

Table 5.24: MNOs in Romania

Although Romania had introduced SIM Registration in 2019, it was abolished in 2020 because the Romanian Constitutional Court declared it as unconstitutional [223].

5.1.24 Slovakia

MCC/MNC*	Provider	Alternative Name	Market Share*	Zero-Rating Program
23101	Orange [224]	Globtel	35.9%	Dátový balík nonstop [225]
23102	Telekom [226]	T-Mobile	30.4%	StreamOn [227]
23106	O2 [228]	Telefonica	27.8%	O2 SMART Paušál [229]
23103	4ka [230]	SWAN Mobile	5.9%	—

*According to messaggio.com [231]

Table 5.25: MNOs in Slovakia

5.1.25 Slovenia

MCC/MNC*	Provider	Alternative Name	Market Share*	Zero-Rating Program
29341	Telekom [232]	Mobitel	40.2%	—
29340	A1 [233]	Si.mobil	31.7%	Play [234]
29370	Telemach [235]	tušmobil	22.3%	—
29364	T-2 [236]		5.8%	—

*According to messaggio.com [237]

Table 5.26: MNOs in Slovenia

5.1.26 Spain

MCC/MNC*	Provider	Alternative Name	Market Share†	Zero-Rating Program
21407	Movistar [238]	Telefónica	30.15%	—
21403	Orange [239]	Amena	24.76%	—
21401	Vodafone [240]	Airtel	22.88%	Vodafone Pass [241]
21404	Yoigo [242]	Grupo MÁSMÓVIL	13.53%	—

*According to messaggio.com [243] †According to Statista [244]

Table 5.27: MNOs in Spain

5.1.27 Sweden

MCC/MNC*	Provider	Alternative Name	Market Share*	Zero-Rating Program
24001	Telia [245]		41.7%	Fri surf Sociala medier [246]
24007	Tele2 [247]		26.6%	Comhem Play [248]
24006	Telenor [249]	Vodafone	18.3%	Telenor Stream [250]
24002	Tre [251]		13.8%	Musikstreaming [252]

*According to messaggio.com [253]

Table 5.28: MNOs in Sweden

5.2 Selected Providers and Tariffs

As already mentioned in Section 4.1.1, we used the results of our market analysis (see Section 5.1) to evaluate the countries where MobileAtlas is deployed and decide which SIM cards to acquire. To quickly get a reasonable amount of coverage, we also weighted in the required effort that is needed to buy the SIM card (e.g., SIM card registration, regional proximity). Thus, we bought SIM cards of the three biggest MNOs of four countries: Austria, Croatia, Romania, and Slovenia.

5.2.1 Austria

Provider	Used Tariff	Included Applications
A1 [63]	A1 SIMply S [254] (incl. A1 Free Stream Chat)	Messenger, Viber, WhatsApp, Snapchat
Magenta [65]	Mobile Youth SIMO S [255] (incl. Magenta Stream Social & Chat)	Facebook, Instagram, WhatsApp, TikTok, Snapchat, Twitter
Drei [67]	Perfect SIM M [256] (incl. MyStream S)	Messenger, WhatsApp, FM4, Ö3, Ö1, Energy, Superfly, Antenne, 886, Kronehit, Radio Arabella

Table 5.29: Selected tariffs in Austria

5.2.2 Croatia

Provider	Used Tariff	Included Applications
Telekom [87]	Simpa XS [257] (incl. Snapchat package*)	Snapchat
A1 [89]	Spikalica [258] (incl. NON STOP SOCIAL)	TikTok, Instagram, WhatsApp, Facebook, Messenger, Snapchat
telemach [91]	—	—

*Alternatively the tariff offers zero-rating packages for the following applications: Whatsapp, Instagram, Facebook + Messenger, Netflix, Youtube, HBO GO, Deezer, Pickbox NOW, MAXtv To Go, Audiomack

Table 5.30: Selected tariffs in Croatia

5.2.3 Slovenia

According to our market analysis in Slovenia (cf. Section 5.1.25), A1 is the only operator that offers a differential pricing tariff (A1 Play). However, A1 Play is only available within A1 Go! tariffs and was therefore not activatable on our purchased prepaid SIM card.

5.2.4 Romania

Provider	Used Tariff	Included Applications
Orange [214]	—*	—
Vodafone [216]	Oferta Roaming 15 [259]	TikTok, WhatsApp, Facebook
Telekom [218]	Optiunea N5† [260]	WhatsApp, Message+

*The desired zero-rating tariff was not available without entering a long lasting (min. 6 month) contract period binding

†Tariff does not support roaming

Table 5.31: Selected tariffs in Romania

5.3 Measurement Results

As described in the previous section, we were able to activate differential pricing offers at seven providers from three different countries.

To identify potential metrics that are used for traffic classification we executed the three experiments (TestNetworkZero, TestNetworZeroCheckSni, TestNetworkZeroCheckIp) that are described in Section 4.3. To be able to identify differences between the domestic and a roaming usage scenario, we executed

- every test
- for every provider
- in every country MobileAtlas currently is deployed in (see Section 4.2.5).

Overall, we've documented more than 200 measurements that were collected within a timespan of two months (August 2021 - October 2021). Although we've conducted many measurements in roamed networks, we only experienced home routed connections and no connections that used a local breakout to the visited network.

5.3.1 Austria

A1

We used a Snapchat user avatar endpoint [261] and queried the resource using HTTPS, HTTP, and HTTP3/QUIC. Table 5.32 shows the results for domestic usage. Furthermore, we got the same results within all foreign countries and therefore can confirm that zero-rating is also applied during roaming. While the traffic classifier can be fooled by a spoofed hostname at HTTP and HTTPS connections (cf. TestNetworkZeroCheckSni), it is also IP-aware since the data packets of the last experiment (cf. TestNetworkZeroCheckIp) were not billed.

Test	HTTPS	HTTP	QUIC	Ctrl
TestNetworkZero	○	○	○	●
TestNetworkZeroCheckSni	○	○	●	●
TestNetworkZeroCheckIp	○	○	○	●

● billed traffic ○ zero-rated traffic

Table 5.32: The Austrian provider A1 uses a both host-based and IP-based classification to identify data traffic that corresponds to Snapchat [261]

At first, we implemented credit checking using SMS-based fund checking because it allowed the most precise unit resolution (0.01 MB instead of 0.01 GB via the website or app). Although the SMS endpoint provides two different quotas for domestic and EU units, the EU quota is only displayed in GB, providing a maximum accuracy of 0.01 GB. Therefore, we also implemented an app-based credit checking approach and had to use a minimum payload size of 10 MB for internationally roamed connections. Because we use binary exponents for our payload size (as described in Section 4.3), one experiment generates about 150MB (10 + 20 + 40 + 80) of data traffic and therefore takes close to 3 hours to finish (using an LTE connection with good reception conditions).

Deutschland - Vodafone

Datum	Beginn	Dauer	Volumen abg./ank.	Zone/Typ	Zielrufnummer/APN	Netto in €
02.09.2021	18:56:36	02:13:24	13,21 MB/47,36 MB	EU Zone Datenvol.	A1.NET	0,0000
02.09.2021	21:10:00	00:23:28	2,87 MB/61,05 MB	EU Zone Datenvol.	A1.NET	0,0000
02.09.2021	21:33:28	00:06:54	793,74 KB/21,25 MB	EU Zone Datenvol.	A1.NET	0,0000
02.09.2021	22:33:10	01:26:50	7,26 MB/15,73 MB	EU Zone Datenvol.	A1.NET	0,0000
03.09.2021	00:00:00	01:03:24	5,90 MB/31,68 MB	EU Zone Datenvol.	A1.NET	0,0000
03.09.2021	01:03:24	00:21:27	3,16 MB/60,76 MB	EU Zone Datenvol.	A1.NET	0,0000
03.09.2021	01:24:51	00:06:19	926,97 KB/21,10 MB	EU Zone Datenvol.	A1.NET	0,0000
03.09.2021	02:16:05	02:16:50	13,03 MB/47,55 MB	EU Zone Datenvol.	A1.NET	0,0000
03.09.2021	04:32:55	00:19:10	3,09 MB/60,82 MB	EU Zone Datenvol.	A1.NET	0,0000
03.09.2021	04:52:05	00:05:41	928,29 KB/21,07 MB	EU Zone Datenvol.	A1.NET	0,0000
03.09.2021	07:06:31	01:43:01	12,03 MB/50,46 MB	EU Zone Datenvol.	A1.NET	0,0000
03.09.2021	08:49:32	00:24:23	3,60 MB/60,32 MB	EU Zone Datenvol.	A1.NET	0,0000
03.09.2021	09:13:55	00:05:37	848,84 KB/21,15 MB	EU Zone Datenvol.	A1.NET	0,0000

Figure 5.1: Unexpected billed data connections during roaming

However, we noticed that the traffic was still not billed correctly. Luckily, the provider offers a connection-based insight into the consumed credit units. As Figure 5.1 shows, the provider lists multiple data connections, although our experiment just uses one persistent data connection. We grouped the documented data connections into the corresponding experiments using red boxes. Thereby, it becomes visible that the provider synthetically "terminates" the connection and issues a bill when roughly 60 MB are consumed. Furthermore, the same behavior occurs at midnight.

To solve this issue, we had to shrink down the data traffic that is consumed by our experiments. Therefore, we separated the payloads (representing the different protocols) into multiple measurements that use less than 60 MB. Thus, we had to execute nine measurements in every roaming country (one for every test and protocol, resulting in 10 + 20 MB payload size for each experiment).

While the consumed data units took about four hours to be billed by the provider during domestic usage, they showed up in billing within 30 minutes when a roamed connection was used.

Magenta

Again, we used a Snapchat user avatar endpoint [261] and queried the resource using HTTPS, HTTP, and HTTP3/QUIC. Implementing credit checking for Magenta was pretty straightforward because the traffic is instantly billed when a data connection is closed, and the REST endpoints that are used by the app provide KB-precise resolution. Paradoxically the minimum billing unit (described in Section 4.2.3) is 50 KB during domestic usage and 1 KB for roamed connections.

Table 5.33 shows the results for domestic usage. The classifier that is used to identify Snapchat traffic relies solely on IP addresses. Also, we got the same results within all foreign countries and therefore can confirm that zero-rating is also applied during roaming.

Test	HTTPS	HTTP	QUIC	Ctrl
TestNetworkZero	○	○	○	●
TestNetworkZeroCheckSni	●	●	●	●
TestNetworkZeroCheckIp	○	○	○	●

● billed traffic ○ zero-rated traffic

Table 5.33: The Austrian provider Magenta uses an IP-based classification approach to identify data traffic that corresponds to Snapchat [261]

Drei

Because our tariff at Drei does not offer zero-rating for Snapchat, we chose a WhatsApp resource [262] to test for differentiation. Although the WhatsApp web server indicated support for HTTP3/QUIC (in the alt-svc header), we did not get any response from the server when an HTTP3 request was issued. We tried out several different client locations (using AWS EC2) and various HTTP3 implementations (Firefox, Chrome, curl, aioquic, etc.), but the problem persisted for several months. When we finally reached out to the WhatsApp support on Twitter [263], the serverside issue was quickly resolved, and we were able to test differentiation using all three protocols (HTTPS, HTTP, and HTTP3/QUIC).

Table 5.34 shows the results for domestic usage. The classifier that is responsible for identifying WhatsApp traffic relies solely on IP addresses. Because we got the same results within all foreign countries, we can confirm that zero-rating is also applied during roaming.

Test	HTTPS	HTTP	QUIC	Ctrl
TestNetworkZero	○	○	○	●
TestNetworkZeroCheckSni	●	●	●	●
TestNetworkZeroCheckIp	○	○	○	●

● billed traffic ○ zero-rated traffic

Table 5.34: The Austrian provider Drei uses an IP-based classification approach to identify data traffic that corresponds to WhatsApp [262]

In contrast to all other tariffs that were evaluated in this thesis and only include international applications, Drei is the only provider that also has regional applications included in its zero-rating offer. Therefore, we examined the classification of traffic that corresponds to the FM4 app[1] that is also part of the zero-rating program.

We determined which resources are requested by the app by recording the corresponding data traffic using PCAPdroid.

As Table 5.35 shows, when testing the apps streaming endpoint [264] using our default methodology (but only HTTPS and HTTP protocol, since the corresponding web server does not support HTTP3/QUIC), no zero-rating could be identified.

Test	HTTPS	HTTP	QUIC	Ctrl
TestNetworkZero	●	●	☒	●
TestNetworkZeroCheckSni	●	●	☒	●
TestNetworkZeroCheckIp	●	●	☒	●

● billed traffic ○ zero-rated traffic ☒ protocol not supported

Table 5.35: The Austrian provider Drei does not zero-rate streaming traffic caused by the FM4 app that is part of its zero-rating offer

Since FM4 also offers a streaming player on their website that uses a different endpoint to retrieve the audio stream, we also checked for zero-rating of the endpoint that is used by the website [265]. Surprisingly, we were able to confirm applied zero-rating when testing the endpoint that is used by their website. Table 5.36 shows that the classifier only applies zero-rating to HTTPS traffic and is not IP aware but solely relies on an

[1] FM4 is an Austrian radio station, and the app offers an audio live-stream to listen to their current program

SNI-based classification approach. Thus, it can be fooled by spoofed SNI header (cf. TestNetworkZeroCheckSni).

Test	HTTPS	HTTP	QUIC	Ctrl
TestNetworkZero	○	●	☒	●
TestNetworkZeroCheckSni	○	●	☒	●
TestNetworkZeroCheckIp	●	●	☒	●

● billed traffic ○ zero-rated traffic ☒ protocol not supported

Table 5.36: The Austrian provider Drei zero-rates streaming traffic caused by the FM4 website

To reaffirm the results of our measurements, we did a short live test where we manually used the FM4 app to stream the radio on a smartphone that was equipped with the corresponding SIM card. We took snapshots of the credit bill before and after the test that confirm that the application's traffic was fully billed (ca. 24 MB for 10 minutes of streaming). Obviously, this can be a huge disadvantage for customers who use the advertised application believing the caused data traffic does not count towards their data bill as it is advertised by the provider.

Because this anomaly made us curious, we examined another application. Again, we identified the relevant resources by capturing the Facebook Messenger apps data traffic. We tested most of the endpoints occuring in our traffic dump ([266, 267, 268, 269, 270, 271, 272, 273]), without finding any zero-rated data traffic. Therefore, supposedly zero-rating does not work accordingly for Facebook Messenger, or at least a substantial part of the data traffic that is caused when using the app is billed by the provider.

5.3.2 Croatia

Telekom

Again, we used a Snapchat user avatar endpoint [261] and queried the resource using HTTPS, HTTP, and HTTP3/QUIC. Table 5.37 shows the results for domestic usage. The classifier that is responsible for identifying Snapchat traffic relies solely on the used hostname (Host- or SNI-header). Thus, the traffic classifier can be fooled by spoofed HTTP and SNI header (cf. TestNetworkZeroCheckSni). However, querying the resource using HTTP3/QUIC resulted in billed traffic. Therefore, we assume that the used classification approach is not configured to work with HTTP3/QUIC.

Again, we used PCAPdroid to record an actual traffic dump of Snapchat data traffic. We verified that the current Snapchat app partly communicates via HTTP3/QUIC. Therefore, we suppose that the operator currently overcharges its customers by billing packets that are part of the zero-rating program.

Test	HTTPS	HTTP	QUIC	Ctrl
TestNetworkZero	○	○	●	●
TestNetworkZeroCheckSni	○	○	●	●
TestNetworkZeroCheckIp	●	●	●	●

● billed traffic ○ zero-rated traffic

Table 5.37: The Croatian provider Telekom uses a hostname-based classification approach to identify data traffic that corresponds to Snapchat [261]

Furthermore, we executed the same experiments in all foreign countries. Table 5.37 shows that zero-rating was not applied during roaming.

Test	HTTPS	HTTP	QUIC	Ctrl
TestNetworkZero	●	●	●	●
TestNetworkZeroCheckSni	●	●	●	●
TestNetworkZeroCheckIp	●	●	●	●

● billed traffic ○ zero-rated traffic

Table 5.38: At Croatian Telekom, traffic that is part of the zero-rating offer (cf. Table 5.37) was fully billed during roaming

A1

Again, we used a Snapchat user avatar endpoint [261] and queried the resource using HTTPS, HTTP, and HTTP3/QUIC. Table 5.39 shows the results for domestic usage. Furthermore, we got the same results within all foreign countries and therefore can confirm that zero-rating is also applied during roaming. While the traffic classifier can be fooled by a spoofed SNI header at HTTPS connections (cf. TestNetworkZeroCheckSni), it does not respect the used hostname when plain HTTP or HTTP3/QUIC is used. Furthermore, it is also IP-aware since the data packets of the last experiment (cf. TestNetworkZeroCheckIp) were not billed.

Test	HTTPS	HTTP	QUIC	Ctrl
TestNetworkZero	○	○	○	●
TestNetworkZeroCheckSni	○	●	●	●
TestNetworkZeroCheckIp	○	○	○	●

● billed traffic ○ zero-rated traffic

Table 5.39: The Croatian provider A1 uses a both SNI-based and IP-based classification to identify data traffic that corresponds to Snapchat [261]

5.3.3 Romania

Vodafone

Because our tariff at Vodafone does not offer zero-rating for Snapchat, we chose a Facebook resource [274] to test for differentiation. Table 5.40 shows the results for domestic usage. While the traffic classifier can be fooled by a spoofed SNI header at HTTPS connections (cf. TestNetworkZeroCheckSni), it does not respect the used hostname when plain HTTP or HTTP3/QUIC is used. Furthermore, it is also IP-aware since the data packets of the last experiment (cf. TestNetworkZeroCheckIp) were not billed.

Test	HTTPS	HTTP	QUIC	Ctrl
TestNetworkZero	○	○	○	●
TestNetworkZeroCheckSni	○	●	●	●
TestNetworkZeroCheckIp	○	○	○	●

● billed traffic ○ zero-rated traffic

Table 5.40: The Romanian provider Vodafone uses a both SNI-based and IP-based classification to identify data traffic that corresponds to Facebook [274]

Furthermore, we executed the same experiments in five out of seven foreign countries. Table 5.37 shows that zero-rating was not applied during roaming. Although the chosen tariff supports international data roaming, and we were able to somehow start a data connection in most cases, roaming did not work very well in practice. We were frequently kicked from the network ("registration denied") and had to deal with aborted data connections during our roaming experiments. To be able to exclude MobileAtlas as a possible cause for the issues, we tested the corresponding tariff on a Nexus 5X in Austria, where we could observe the same behavior (restless hopping between providers, no persistent data connection). We were not able to successfully perform measurements in Germany because the modem was not able to successfully register to the cellular network. In Belgium, we were able to establish a data connection but experienced a packet loss of more than 65%, which did not make it possible to successfully transmit the payloads of our measurements. In the other foreign countries (Austria, Croatia, Finland, Slovakia, Slovenia), we also experienced some issues (e.g., in Austria, the data connection always automatically terminated after 185 seconds) but were able to successfully execute the experiment with some tweaks (e.g., by shrinking the minimum payload size to make the experiment finish within time). The results of our measurements in those five foreign countries can be seen in Table 5.40. Zero-rating was not applied during roaming.

Telekom

Again, we used a Snapchat user avatar endpoint [261] and queried the resource using HTTPS, HTTP, and HTTP3/QUIC. Since Telekom does not offer any zero-rating tariffs that support data roaming, we were only able to test it in a domestic usage

Test	HTTPS	HTTP	QUIC	Ctrl
TestNetworkZero	●	●	●	●
TestNetworkZeroCheckSni	●	●	●	●
TestNetworkZeroCheckIp	●	●	●	●

● billed traffic ○ zero-rated traffic

Table 5.41: At Romanian Vodafone, traffic that is part of the zero-rating offer (cf. Table 5.40) was fully billed during roaming

scenario. Table 5.42 shows the results. The classifier that is responsible for identifying Snapchat traffic relies solely on the used hostname (Host- or SNI-header). Thus, the traffic classifier can be fooled by a spoofed hostname at HTTP and HTTPS connections (cf. TestNetworkZeroCheckSni). However, querying the resource using HTTP3/QUIC resulted in billed traffic. Therefore, we assume that the used classification approach is not configured to work with HTTP3/QUIC. Because the results are equal to those of Croatian Telekom, further implications are described in Section 5.3.2.

Test	HTTPS	HTTP	QUIC	Ctrl
TestNetworkZero	○	○	●	●
TestNetworkZeroCheckSni	○	○	●	●
TestNetworkZeroCheckIp	●	●	●	●

● billed traffic ○ zero-rated traffic

Table 5.42: The Romanian provider Telekom uses a hostname-based classification approach to identify data traffic that corresponds to Snapchat [261]

5.4 Summarized Results

Table 5.43 shows a summary of the classification characteristics we've found measuring zero-rating at the tested providers.

Potential classification issues that we've found are

- zero-rating is not applied for HTTP3/QUIC communication at Croatian and Romanian Telekom,
- zero-rating is not applied within roamed connections at Croatian Telekom and Romanian Vodafone,
- zero-rating of one or more apps (e.g., FM4) does not work at Austrian Drei.

Country	Provider	Classifier	Supports QUIC	Supports Roaming
Austria	A1	IP, DPI	●	●
	Magenta	IP	●	●
	Drei	IP, DPI	●	●
Croatia	Telekom	DPI	○	○
	A1	IP, DPI	●	●
Romania	Vodafone	IP, DPI	●	○
	Telekom	DPI	○	☒

● yes ○ no ☒ not available

Table 5.43: Summarized results of tested providers

Therefore, we've identified potentially problematic behavior at more than a half (4/7) of tested providers.

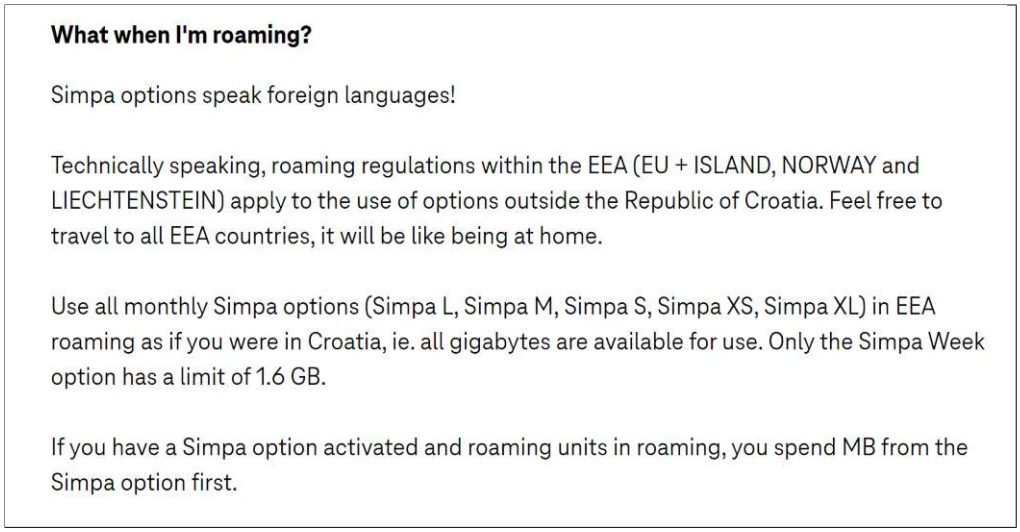
CHAPTER 6

Discussion

This thesis focuses on a technical analysis of differential pricing practices at European mobile network providers. Beyond the plain results of our measurements, various other issues were revealed during our work.

We've noticed that various providers only apply zero-rating offers during domestic usage and normally bill all consumed units at roamed data connections. This is a known practice, and some operators in Germany were forced by the responsible NRA to change this behavior [4, 5]. Whether this practice complies with EU net neutrality laws has to be ultimately decided in court. However, we still want to comment on it from a user's perspective. At providers who do not apply zero-rating abroad, we tried to find statements (e.g., within tariff FAQs or even specific contract conditions) that mention this special treatment for roamed connections. However, we did not find any comments about it. This lack of clarification and transparency can be a huge disadvantage for customers when zero-rating applications are used within roaming and consumed units are suddenly billed. Even worse, Croatian Telekom claims that the used tariff "does speak foreign languages" and "can be used like at home" (as can be seen in Figure 6.1), although we noticed that zero-rating was not applied during roaming.

Moreover, this is not the only case where a lack of transparency results in a potential contract violation. The Austrian provider Drei claims to zero-rate the FM4 (radio streaming) app. While the stream that is used within the app is fully billed, we found an alternative streaming source (from the radio's website) to be actually zero-rated instead. We suppose that this was not done on purpose, but possibly because the classification rules were not implemented correctly or because the app was using the website's streaming endpoint in earlier versions, and the classifier was not updated accordingly. However, the consequences for a customer are crucial when the FM4 app is used to listen to the radio and the caused data traffic is wrongfully billed.



What when I'm roaming?

Simpa options speak foreign languages!

Technically speaking, roaming regulations within the EEA (EU + ISLAND, NORWAY and LIECHTENSTEIN) apply to the use of options outside the Republic of Croatia. Feel free to travel to all EEA countries, it will be like being at home.

Use all monthly Simpa options (Simpa L, Simpa M, Simpa S, Simpa XS, Simpa XL) in EEA roaming as if you were in Croatia, ie. all gigabytes are available for use. Only the Simpa Week option has a limit of 1.6 GB.

If you have a Simpa option activated and roaming units in roaming, you spend MB from the Simpa option first.

Figure 6.1: Roaming Terms for Croatian Telekom's Simpa Tariffs [257]

We noticed that another problem arises when protocols or applications evolve over time and providers do not update classification rules accordingly. Application providers that are part of a zero-rating program should provide the operator with current protocol specification details and also notify the operator before making relevant application changes. However, we do not have any further insights. Several operators did not successfully classify our tested HTTP3/QUIC traffic, and we noticed that some applications (e.g., Snapchat, WhatsApp, etc.) already communicate over HTTP3 with certain endpoints. Therefore, we suppose that the corresponding HTTP3 traffic is wrongfully billed as well and that the defined process for application changes does not work very well in practice. To end the wild west of zero-rating and make traffic classification comprehensible and verifiable by a third party (e.g., NRAs), the corresponding actors should be obliged to publish the relevant data. This includes the used classification rules, as well as an up-to-date blueprint of the application's communication endpoints that were provided by the application creator and used to implement traffic classification.

Operators often try to make exceptions for third-party content (e.g., an advertisement) that is loaded and displayed within zero-rating apps. This makes it hard for customers to fully comprehend what is included within the offered tariffs. Moreover, many customers use Android or iOS to view how much data traffic certain apps consume and therefore make wrong assumptions on the data that is still left for consummation (especially when zero-rated traffic was not correctly billed by a provider). Although every provider usually offers some way to retrieve the general data quota (e.g., via a specific provider app that needs registration), there is no uniform interface that allows more detailed insights (e.g., an enumeration of single data connections with accurate traffic usage). This would help customers to understand and track their used data or find anomalies in billing and make consumption comparable across different providers.

To summarize, we think that customers would benefit from a more unified behavior across all providers (e.g., in terms of a homogeneous interface for billed units or zero-rating behavior during roaming). Furthermore, providers should be more transparent about their classification practices and therefore publish the metrics that are used for classification.

6.1 Limitations and Future Work

Because this study was conducted within tight funding and time constraints, we had to limit the scope and several parameters to a meaningful measure.

Tested Applications and Endpoints Although providers often enroll many different applications to their zero-rating offers, we only tested a fractional part of them. Furthermore, one application usually communicates with many different endpoints that sometimes are distributed across different servers or locations (especially when CDNs are involved). For a specific service, we usually manually picked the first endpoint that showed signs of zero-rating and then conducted our measurements for a more detailed evaluation.

Measurement Execution and Implementation Currently, executing a measurement still requires human intervention. We aim to implement measurement planning and scheduling via our management server. This obviously boosts efficiency and makes testing for a large amount of applications and endpoints feasible. Furthermore, we plan to implement more complex measurements. Although the tests that were executed within this work already provide valuable insights and can be used to successfully detect the used classification metrics, our approach might not provide accurate results when the classifier uses fingerprinting or anomaly detection (e.g., by considering packet flow, bit-rate, etc.). Therefore, using a record-replay approach or tunneling real-world traffic from a specific application via our test platform would provide further insights that are worth studying. Furthermore, we currently rely on automatic network operator selection during roaming. Often there are multiple possible roaming partners in one country that technically could lead to different measurement results. Last but not least, this study focuses on detecting economic differentiation. However, the MobileAtlas measurement platform could be used to analyze other parameters (rate limiting, traffic manipulation, censorship, QoS/QoE, etc.) in mobile networks and roaming environments.

Tested Countries and Providers Although compared to previous measurement approaches MobileAtlas reduces the required effort for roaming measurements, we can only measure tariffs that are active on one of our SIM cards. However, due to SIM registration laws, language barriers, and regional proximity, the process of acquiring foreign SIM cards is very cumbersome. Moreover, specific tariffs are only available within long-term contracts (e.g., 24 months binding), which makes them infeasible (or very expensive) to acquire and evaluate. Furthermore, the

MobileAtlas platform is still in pilot phase and only deployed in eight European countries, which obviously limits our measurements to these countries. Therefore, we plan to increase coverage of the platform by building and deploying probes to multiple countries across Europe.

To summarize, we plan to continue working on mobile network measurements and keeping up our efforts to improve and extend the MobileAtlas measurement framework. To encourage collaborative participation, we publish the MobileAtlas source code and hardware description along with all measurement artifacts that were collected during this study[1]. Besides support from the community, we hope for additional support in terms of funding that would help us to promote MobileAtlas and allow us to buy even more foreign SIM cards for further analysis and evaluation.

[1] https://mobileatlas.eu/thesis

CHAPTER 7

Conclusion

In this thesis, we have shown that the mobile network ecosystem, and in particular, differential pricing, is an unstructured and intransparent mess and that current zero-rating practices can have serious implications regarding consumer protection (i.e., incorrect billing). We conducted an EU-wide market analysis that provides a brief overview of legal regulations, relevant market players, and existing zero-rating tariffs. We developed MobileAtlas, a novel measurement platform for international roaming measurements that focuses on fine-grained measurements and geographically decouples the SIM card from the cellular modem. We used MobileAtlas, to characterize the zero-rating behavior at seven operators from three different countries by taking measurements in eight target countries (one domestic and seven international roaming usage scenarios). Thus, our work introduces a powerful tool to independently audit network operators and helps to get a better insight into current provider practices, particularly regarding zero-rating and international roaming.

Appendix

Probe Part List and Costs

Component	Model	Cost
Single-board computer	Raspberry Pi 4B, 4GB RAM	60€
Power supply	Official Raspberry Pi Power Supply	10€
SD card	Samsung Evo Plus 128GB	15€
Modem	Quectel EG25-G (mPCIe)	75€
Modem adapter	Sixfab Raspberry Pi LTE Base HAT	44€
Antenna	W6113B0100 [1]	10€
Case	Sixfab Raspberry Pi IP54 Case	80€
Misc	Selfmade SIM adapter, Network cable, etc.	5€
Total		299€

[1] Any antenna that supports the corresponding frequencies should work equally well.

Table 1: Sample part list and pricing for one measurement probe

List of Figures

List of Tables

List of Algorithms

Acronyms

AES Advanced Encryption Standard. 5

APDU Application Protocol Data Unit. 5, 22

ATR Answer To Reset. 22

BEREC Body of European Regulators for Electronic Communications. 1

DPI Deep Packet Inspection. 8

ESNI Encrypted SNI. 9

GPIO General-Purpose Input/Output. 19

GSM Global System for Mobile Communications. 5

HR Home-Routed Roaming. 6

HTTP Hypertext Transfer Protocol. 7

HTTPS HTTP Secure. 7

IHBO IPX Hub Breakout. 6

IP Internet Protocol. 6

ISP Internet Service Provider. 7

LR Local Breakout. 6

LTE Long Term Evolution. 5

MBIM Mobile Broadband Interface Model. 6

MNO Mobile Network Operator. 1, 17

MNVO Mobile Network Virtual Operator. 18

NRA National Regulatory Authority. 1

PPP Point-to-Point Protocol. 6

PPS Protocol and Parameter Selection. 22

QMI Qualcomm MSM Interface. 6

QUIC Quick UDP Internet Connections. 7

REST Representational State Transfer. 7

SIM Subscriber Identity Module. 5

SNI Server Name Identification. 9

TCP Transmission Control Protocol. 8

TLS Transport Layer Security. 7

TTL Time To Live. 8

UART Universal Asynchronous Receiver Transmitter. 22

UDP User Datagram Protocol. 8

UMTS Universal Mobile Telecommunications System. 5

USART Universal Synchronous Asynchronous Receiver Transmitter. 22

USIM Universal Subscriber Identity Module. 5

WTX Waiting Time eXtensions. 22

Bibliography

[1] Mobile vs. Desktop Internet Usage. https://www.broadbandsearch.net/blog/mobile-desktop-internet-usage-statistics. Accessed: 2020-08-19.

[2] BEREC. International Roaming BEREC Benchmark Data Report April 2019 – September 2019. https://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/9031-international-roaming-berec-benchmark-da_0.pdf, March 2020. Accessed: 2020-07-01.

[3] BEREC. International Roaming BEREC Benchmark Data Report April 2019 – September 2019. https://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/8840-report-on-the-implementation-of-regulati_0.pdf, October 2019. Accessed: 2020-07-01.

[4] Bundesnetzagentur untersagt Details des "StreamOn"-Tarifs der Telekom. https://heise.de/-3852918, October 2017. Accessed: 2020-07-01.

[5] Zero Rating: Regulierer grätscht auch bei Vodafone Pass rein. https://heise.de/-4079923, June 2018. Accessed: 2020-07-01.

[6] Anna Maria Mandalari, Andra Lutu, Ana Custura, Ali Safari Khatouni, Özgü Alay, Marcelo Bagnulo, Vaibhav Bajpai, Anna Brunstrom, Jörg Ott, Marco Mellia, and Gorry Fairhurst. Experience: Implications of roaming in europe. In *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking*, MobiCom '18, pages 179–189, New York, NY, USA, 2018. ACM.

[7] Google IPv6 Statistics. https://www.google.com/intl/en/ipv6/statistics.html. Accessed: 2020-09-04.

[8] Sandvine. Identifying and measuring internet traffic: Techniques and considerations. Industry whitepaper, Sandvine, 2015.

[9] Marcel Dischinger, Massimiliano Marcon, Saikat Guha, P Krishna Gummadi, Ratul Mahajan, and Stefan Saroiu. Glasnost: Enabling End Users to Detect Traffic Differentiation. In *Networked Systems Design and Implementation (NSDI)*, pages 405–418. USENIX, 2010.

[10] Ying Zhang, Zhuoqing Morley Mao, and Ming Zhang. Detecting Traffic Differentiation in Backbone ISPs with NetPolice. In *Internet Measurement Conference (IMC)*, pages 103–115. ACM, 2009.

[11] Vitali Bashko, Nikolay Melnikov, Anuj Sehgal, and Jürgen Schönwälder. BonaFide: A Traffic Shaping Detection Tool for Mobile Networks. In *International Symposium on Integrated Network Management (IM)*, pages 328–335. IFIP/IEEE, 2013.

[12] Utkarsh Goel, Ajay Miyyapuram, Mike P Wittie, and Qing Yang. Mitate: Mobile internet testbed for application traffic experimentation. In *International Conference on Mobile and Ubiquitous Systems: Computing, Networking, and Services*, pages 224–236. Springer, 2013.

[13] Arash Molavi Kakhki, Abbas Razaghpanah, Anke Li, Hyungjoon Koo, Rajesh Golani, David Choffnes, Phillipa Gill, and Alan Mislove. Identifying traffic differentiation in mobile networks. In *Proceedings of the 2015 Internet Measurement Conference*, pages 239–251, 2015.

[14] Fangfan Li, Arian Akhavan Niaki, David Choffnes, Phillipa Gill, and Alan Mislove. A large-scale analysis of deployed traffic differentiation practices. In *Proceedings of the ACM Special Interest Group on Data Communication*, pages 130–144. 2019.

[15] Wehe. `https://dd.meddle.mobi/`. Accessed: 2021-08-27.

[16] Tobias Flach, Pavlos Papageorge, Andreas Terzis, Luis Pedrosa, Yuchung Cheng, Tayeb Karim, Ethan Katz-Bassett, and Ramesh Govindan. An internet-wide analysis of traffic policing. In *Proceedings of the 2016 ACM SIGCOMM Conference*, pages 468–482, 2016.

[17] Arturo Filasto and Jacob Appelbaum. Ooni: Open observatory of network interference. In *Presented as part of the 2nd USENIX Workshop on Free and Open Communications on the Internet*, Bellevue, WA, 2012.

[18] Open Observatory of Network Interference. `https://ooni.org/`. Accessed: 2021-08-27.

[19] Simurgh Aryan, Homa Aryan, and J Alex Halderman. Internet censorship in iran: A first look. In *3rd USENIX Workshop on Free and Open Communications on the Internet (FOCI 13)*, 2013.

[20] Nicholas Weaver, Christian Kreibich, and Vern Paxson. Redirecting DNS for Ads and Profit. In *USENIX Workshop on Free and Open Communications on the Internet (FOCI)*, San Francisco, CA, USA, August 2011.

[21] Wilfried Mayer, Thomas Schreiber, and Edgar Weippl. A framework for monitoring net neutrality. In *Proceedings of the 13th International Conference on Availability, Reliability and Security*, pages 1–10, 2018.

[22] Gabi Nakibly, Jaime Schcolnik, and Yossi Rubin. Website-targeted false content injection by network operators. In *25th USENIX Security Symposium USENIX Security 16*, pages 227–244, 2016.

[23] RIPE NCC Staff. Ripe atlas: A global internet measurement network. *Internet Protocol Journal*, 18(3), 2015.

[24] RIPE Network Coordination Centre. `https://atlas.ripe.net/`. Accessed: 2021-08-27.

[25] Collin Anderson, Philipp Winter, et al. Global network interference detection over the RIPE atlas network. In *4th USENIX Workshop on Free and Open Communications on the Internet (FOCI 14)*, 2014.

[26] Ruwaifa Anwar, Haseeb Niaz, David Choffnes, Ítalo Cunha, Phillipa Gill, and Ethan Katz-Bassett. Investigating interdomain routing policies in the wild. In *Proceedings of the 2015 Internet Measurement Conference*, pages 71–77, 2015.

[27] Ben Jones, Nick Feamster, Vern Paxson, Nicholas Weaver, and Mark Allman. Detecting dns root manipulation. In *International Conference on Passive and Active Network Measurement*, pages 276–288. Springer, 2016.

[28] Fangfan Li, Arash Molavi Kakhki, David Choffnes, Phillipa Gill, and Alan Mislove. Classifiers unclassified: An efficient approach to revealing ip traffic classification rules. In *Proceedings of the 2016 Internet Measurement Conference*, pages 239–245, 2016.

[29] Arash Molavi Kakhki, Fangfan Li, David Choffnes, Ethan Katz-Bassett, and Alan Mislove. Bingeon under the microscope: Understanding t-mobiles zero-rating implementation. In *Proceedings of the 2016 workshop on QoE-based Analysis and Management of Data Communication Networks*, pages 43–48, 2016.

[30] Younghwan Go, EunYoung Jeong, Jongil Won, Yongdae Kim, Denis Foo Kune, and KyoungSoo Park. Gaining control of cellular traffic accounting by spurious tcp retransmission. In *NDSS*, 2014.

[31] Chi-Yu Li, Guan-Hua Tu, Chunyi Peng, Zengwen Yuan, Yuanjie Li, Songwu Lu, and Xinbing Wang. Insecurity of voice solution volte in lte mobile networks. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pages 316–327, 2015.

[32] Özgü Alay, Andra Lutu, David Ros, Rafael Garcia, Vincenzo Mancuso, Audun Fosselie Hansen, Anna Brunstrom, Marco Ajmone Marsan, and Hakon Lonsethagen. MONROE: Measuring Mobile Broadband Networks in Europe. In *Workshop on Research and Applications of Internet Measurements (RAIM)*. IRTF & ISOC, 2015.

[33] Özgü Alay, Andra Lutu, Rafael García, Miguel Peón-Quirós, Vincenzo Mancuso, Thomas Hirsch, Tobias Dely, Jonas Werme, Kristian Evensen, Audun Hansen, et al. Measuring and Assessing Mobile Broadband Networks with MONROE. In *International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, pages 1–3. IEEE, 2016.

[34] Blank map of Europe, Licensed under Creative Commons Attribution-ShareAlike 3.0 Unported (CC BY-SA 3.0) [275]. https://commons.wikimedia.org/wiki/File:Blank_map_of_Europe_cropped.svg. Accessed: 2021-10-10.

[35] GSMA. Access to Mobile Services and Proof of Identity 2021. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2021/04/Digital-Identity-Access-to-Mobile-Services-and-Proof-of-Identity-2021_SPREADs.pdf, April 2021. Accessed: 2020-09-22.

[36] RTR. https://www.rtr.at/TKP/Telecommunications_and_Postal_Division.en.html. Accessed: 2021-09-25.

[37] BIPT. https://www.bipt.be/consumers. Accessed: 2021-09-25.

[38] CRC. https://crc.bg/en. Accessed: 2021-09-25.

[39] HAKOM. https://www.hakom.hr/. Accessed: 2021-09-25.

[40] OCECPR. https://ocecpr.ee.cy/. Accessed: 2021-09-25.

[41] CTU. https://www.ctu.eu/. Accessed: 2021-09-25.

[42] DBA. https://danishbusinessauthority.dk/. Accessed: 2021-09-25.

[43] ETRA. https://www.ttja.ee/en. Accessed: 2021-09-25.

[44] FICORA. https://www.traficom.fi/en/. Accessed: 2021-09-25.

[45] ARCEP. https://en.arcep.fr/. Accessed: 2021-09-25.

[46] BNetzA. https://www.bundesnetzagentur.de/EN/Areas/Telecommunications/telecommunications-node.html. Accessed: 2021-09-25.

[47] EETT. https://www.eett.gr/opencms/opencms/EETT_EN. Accessed: 2021-09-25.

[48] NMHH. https://english.nmhh.hu/. Accessed: 2021-09-25.

[49] ComReg. https://www.comreg.ie/. Accessed: 2021-09-25.

[50] AGCOM. https://www.agcom.it/. Accessed: 2021-09-25.

[51] SPRK. https://www.sprk.gov.lv/. Accessed: 2021-09-25.

[52] RRT. https://www.rrt.lt/. Accessed: 2021-09-25.

[53] ILR. https://web.ilr.lu/FR/ILR. Accessed: 2021-09-25.

[54] MCA. https://www.mca.org.mt/. Accessed: 2021-09-25.

[55] ACM. https://www.acm.nl/en. Accessed: 2021-09-25.

[56] UKE. https://en.archiwum.uke.gov.pl/. Accessed: 2021-09-25.

[57] ANACOM. https://www.anacom.pt/render.jsp?languageId=1. Accessed: 2021-09-25.

[58] ANCOM. https://www.ancom.ro/en/. Accessed: 2021-09-25.

[59] RU. https://www.teleoff.gov.sk/regulatory-authority-for-electronic-communications-and-postal-services/. Accessed: 2021-09-25.

[60] AKOS. https://www.akos-rs.si/en/. Accessed: 2021-09-25.

[61] CNMC. https://www.cnmc.es/en. Accessed: 2021-09-25.

[62] PTS. https://www.pts.se/en-gb/. Accessed: 2021-09-25.

[63] A1 (Austria). https://www.a1.net/. Accessed: 2021-08-25.

[64] A1 Free Stream. https://www.a1.net/free-stream. Accessed: 2021-08-25.

[65] Magenta (Austria). https://www.magenta.at/. Accessed: 2021-08-25.

[66] Magenta Stream. https://www.magenta.at/magentastream. Accessed: 2021-08-25.

[67] Drei (Austria). https://www.drei.at/de/privat/. Accessed: 2021-08-25.

[68] Drei MyStream. https://www.drei.at/de/privat/telefonie/jugend-tarife/mystream.html. Accessed: 2021-08-25.

[69] RTR MNC. https://www.rtr.at/TKP/service/rufnummernsuche/SKPzugeteilt.de.html. Accessed: 2021-08-25.

[70] RTR Telekom Monitor Q2 2020. https://www.rtr.at/TKP/aktuelles/publikationen/publikationen/Datenvisualisierung/telekom-monitor-q22020-daten.de.html. Accessed: 2021-08-25.

[71] Proximus (Belgium). https://www.proximus.be/en/. Accessed: 2021-08-25.

[72] Proximus Epic. https://www.proximus.be/epic/en/id_zwpe_p/makeitepic/mobile.html. Accessed: 2021-08-25.

[73] Orange (Belgium). https://www.orange.be/. Accessed: 2021-08-25.

[74] BASE (Belgium). https://www.base.be/en/private.html. Accessed: 2021-08-25.

[75] Messaggio: Market Overview Belgium. https://messaggio.com/messaging/belgium/. Accessed: 2021-08-25.

[76] BIPT Annual Report 2020. https://www.bipt.be/operators/publication/annual-report-2020. Accessed: 2021-08-25.

[77] Telenet Free-G. https://www2.telenet.be/nl/klantenservice/free-g/. Accessed: 2021-08-25.

[78] A1 (Bulgaria). https://www.a1.bg/bg?home. Accessed: 2021-08-25.

[79] A1 One Traffic pass. https://www.a1.bg/a1-one-unlimited. Accessed: 2021-08-25.

[80] Telenor (Bulgaria). https://www.telenor.bg/. Accessed: 2021-08-25.

[81] Telenor Postpaid Traffic pass. https://www.telenor.bg/plans/postpaid-plans/add-ons. Accessed: 2021-08-25.

[82] VIVAcom (Bulgaria). https://www.vivacom.bg/bg. Accessed: 2021-08-25.

[83] Ti.com (Bulgaria). https://www.ticom.bg/. Accessed: 2021-08-25.

[84] Bulsatcom (Bulgaria). https://www.bulsat.com/. Accessed: 2021-08-25.

[85] Messaggio: Market Overview Bulgaria. https://messaggio.com/messaging/bulgaria/. Accessed: 2021-08-25.

[86] Alertify: Market Overview Bulgaria. https://alertify.eu/europe-telecoms/bulgaria-telecom-market/. Accessed: 2021-08-25.

[87] Hrvatski Telekom (Croatia). https://www.hrvatskitelekom.hr/. Accessed: 2021-08-25.

[88] Hrvatski Telekom StreamOn. https://www.hrvatskitelekom.hr/dodatne-usluge/stream-on. Accessed: 2021-08-25.

[89] A1 (Croatia). https://www.a1.hr/. Accessed: 2021-08-25.

[90] A1 NON STOP SOCIAL. https://www.a1.hr/privatni/mobiteli/a1-na-bonove. Accessed: 2021-08-25.

[91] telemach (Croatia). https://telemach.hr/. Accessed: 2021-08-25.

[92] Messaggio: Market Overview Croatia. https://messaggio.com/messaging/croatia/. Accessed: 2021-08-25.

[93] epic (Cyprus). https://www.epic.com.cy/en/page/start/home. Accessed: 2021-08-25.

[94] Cyta (Cyprus). https://www.cyta.com.cy/personal/en. Accessed: 2021-08-25.

[95] PrimeTel (Cyprus). https://primetel.com.cy/. Accessed: 2021-08-25.

[96] Messaggio: Market Overview Cyprus. https://messaggio.com/messaging/cyprus/. Accessed: 2021-08-25.

[97] MNT Facebook Zero. https://web.archive.org/web/20190606044329/http://www.mtn.com.cy/en/facebookzero/. Accessed: 2021-08-25.

[98] T-Mobile (Czech Republic). https://www.t-mobile.cz/osobni. Accessed: 2021-08-25.

[99] O2 (Czech Republic). https://www.o2.cz/osobni/en/. Accessed: 2021-08-25.

[100] Vodafone (Czech Republic). https://www.vodafone.cz/en/. Accessed: 2021-08-25.

[101] Vodafone Pass. https://www.vodafone.cz/en/internet/vodafone-pass2. Accessed: 2021-08-25.

[102] Messaggio: Market Overview Czech Republic. https://messaggio.com/messaging/czech-republic/. Accessed: 2021-08-25.

[103] Czech SteamOn bites the dust. https://www.telcotitans.com/deutsche-telekomwatch/t-mobile-czech-republic-streamon-bites-the-dust/724.article. Accessed: 2021-08-25.

[104] TDC (Denmark). https://yousee.dk/. Accessed: 2021-08-25.

[105] YouSee Music. https://yousee.dk/mobil/abonnementer/fri/. Accessed: 2021-08-25.

[106] Telenor (Denmark). https://www.telenor.dk/. Accessed: 2021-08-25.

[107] Telia (Denmark). https://www.telia.dk/. Accessed: 2021-08-25.

[108] 3 (Denmark). https://www.3.dk/. Accessed: 2021-08-25.

[109] Messaggio: Market Overview Denmark. https://messaggio.com/messaging/denmark/. Accessed: 2021-08-25.

[110] Telia (Estonia). https://www.telia.ee/era. Accessed: 2021-08-25.

[111] Telia Spotify Offer. https://www.telia.ee/era/mobiil/mobiilne-elu. Accessed: 2021-08-25.

[112] Elisa (Estonia). https://www.elisa.ee/. Accessed: 2021-08-25.

[113] Tele2 (Estonia). https://tele2.ee/. Accessed: 2021-08-25.

[114] Messaggio: Market Overview Estonia. https://messaggio.com/messaging/estonia/. Accessed: 2021-08-25.

[115] Elisa (Finland). https://elisa.fi. Accessed: 2021-08-25.

[116] Telia (Finland). https://www.telia.fi/english. Accessed: 2021-08-25.

[117] DNA (Finland). https://www.dna.fi/. Accessed: 2021-08-25.

[118] Ålcom (Finland). https://www.alcom.ax/. Accessed: 2021-08-25.

[119] FICORA: Approved Mobile Network Codes (MNC). https://www.traficom.fi/en/communications/broadband-and-telephone/approved-mobile-network-codes-mnc. Accessed: 2021-08-25.

[120] Statista: Market Share of Telecommunication Providers in Finland. https://www.statista.com/statistics/733154/market-share-of-telecommunication-providers-in-finland/. Accessed: 2021-08-25.

[121] Facebook Zero for Emerging Markets. https://www.engadget.com/2010-05-19-facebook-launches-free-mobile-access-site-for-emerging-markets.html. Accessed: 2021-08-25.

[122] Orange (France). https://www.orange.fr/portail. Accessed: 2021-08-25.

[123] SFR (France). https://www.sfr.fr/. Accessed: 2021-08-25.

[124] Bouygues (France). https://www.bouyguestelecom.fr/. Accessed: 2021-08-25.

[125] Bouygues B.tv. https://www.bouyguestelecom.fr/option-mobile/btv. Accessed: 2021-08-25.

[126] Free Mobile (France). https://www.free.fr/. Accessed: 2021-08-25.

[127] Messaggio: Market Overview France. https://messaggio.com/messaging/france/. Accessed: 2021-08-25.

[128] Vodafone (Germany). https://www.vodafone.de/. Accessed: 2021-08-25.

[129] Vodafone Pass. https://www.vodafone.de/privat/service/vodafone-pass.html. Accessed: 2021-08-25.

[130] Telekom (Germany). https://www.telekom.de/. Accessed: 2021-08-25.

[131] Telekom StreamOn. https://www.telekom.de/unterwegs/tarife-und-optionen/streamon. Accessed: 2021-08-25.

[132] O2 (Germany). https://www.o2online.de. Accessed: 2021-08-25.

[133] Messaggio: Market Overview Germany. https://messaggio.com/messaging/germany/. Accessed: 2021-08-25.

[134] Teilnehmerentwicklung im Mobilfunk. https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Marktbeobachtung/Deutschland/Mobilfunkteilnehmer/Mobilfunkteilnehmer_node.html. Accessed: 2021-08-25.

[135] Cosmote (Greece). http://www.cosmote.gr/. Accessed: 2021-08-25.

[136] Cosmote Chat Now. https://www.cosmote.gr/cs/cosmote/gr/giga_max_chat_now.html. Accessed: 2021-08-25.

[137] Vodafone (Greece). http://www.vodafone.gr/. Accessed: 2021-08-25.

[138] Vodafone Pass. https://www.vodafone.gr/eshop/vodafone-mobile/vodafone-pass/. Accessed: 2021-08-25.

[139] Wind (Greece). http://www.wind.gr/. Accessed: 2021-08-25.

[140] Messaggio: Market Overview Greece. https://messaggio.com/messaging/greece/. Accessed: 2021-08-25.

[141] Archive of Wind QSurf (WhatsApp Zero-Rating) Tariff. https://web.archive.org/web/20180828130426/https://www.wind.gr/gr/q/paketa/paketa-data/q-surf/. Accessed: 2021-08-25.

[142] Telekom (Hungary). https://www.telekom.hu/. Accessed: 2021-08-25.

[143] ZENE OPCIÓ. https://www.telekom.hu/lakossagi/szolgaltatasok/mobil/havi-dijas-mobil-dijcsomagok/zene. Accessed: 2021-08-25.

[144] Korlátlan alkalmazások. https://www.telekom.hu/lakossagi/szolgaltatasok/internet/mobilinternet/havi-dijas-csomagok/net-4GB-2020. Accessed: 2021-08-25.

[145] Telenor (Hungary). https://en.telenor.hu/. Accessed: 2021-08-25.

[146] Telenor Pass. https://en.telenor.hu/hellochat-prepaid. Accessed: 2021-08-25.

[147] Vodafone (Hungary). https://www.vodafone.hu/. Accessed: 2021-08-25.

[148] Vodafone Pass. https://www.vodafone.hu/english/goodthings/vodafone-pass. Accessed: 2021-08-25.

[149] DIGIMobil (Hungary). https://digi.hu/. Accessed: 2021-08-25.

[150] Messaggio: Market Overview Hungary. https://messaggio.com/messaging/hungary/. Accessed: 2021-08-25.

[151] 3 (Ireland). https://www.three.ie/. Accessed: 2021-08-25.

[152] Vodafone (Ireland). https://vodafone.ie/. Accessed: 2021-08-25.

[153] eir (Ireland). https://www.eir.ie/. Accessed: 2021-08-25.

[154] Messaggio: Market Overview Ireland. https://messaggio.com/messaging/ireland/. Accessed: 2021-08-25.

[155] ComReg Zero-Rating of Healthcare and Educational Content during COVID-19. https://www.comreg.ie/comreg-welcomes-telecoms-industry-commitments-to-assist-consumers-during-covid-19/. Accessed: 2021-08-25.

[156] TIM (Italy). https://www.tim.it/. Accessed: 2021-08-25.

[157] GIGA ILLIMITATI CARD Social and Chat. https://www.tim.it/fisso-e-mobile/mobile/social-chat-card. Accessed: 2021-08-25.

[158] Vodafone (Italy). https://www.vodafone.it. Accessed: 2021-08-25.

[159] Vodafone Pass. https://www.vodafone.it/portal/Privati/Tariffe-e-Prodotti/Tariffe/Giga-per-le-app. Accessed: 2021-08-25.

[160] WINDTRE (Italy). https://www.windtre.it/. Accessed: 2021-08-25.

[161] Iliad (Italy). https://www.iliad.it/. Accessed: 2021-08-25.

[162] Messaggio: Market Overview Italy. https://messaggio.com/messaging/italy/. Accessed: 2021-08-25.

[163] Statista: Italy Market Share Mobile Operators. https://www.statista.com/statistics/548650/market-share-of-mobile-operator-revenue-in-italy/. Accessed: 2021-08-25.

[164] Windtre discontinued Zero-Rating. https://www.webnews.it/2017/03/22/agcom-diffida-wind-tre-sullo-zero-rating/. Accessed: 2021-08-25.

[165] Italy: Zero-Rating of Educational Content during COVID-19. https://paschinilinussio.edu.it/2020/11/29/tariffe-zero-rating-per-la-didattica-da-casa/. Accessed: 2021-08-25.

[166] LMT (Latvia). https://lmt.lv/. Accessed: 2021-08-25.

[167] Tele2 (Latvia). https://tele2.lv/. Accessed: 2021-08-25.

[168] Bite (Latvia). https://bite.lv/. Accessed: 2021-08-25.

[169] Neierobežots Internets Aplikācijām. https://www.bite.lv/lv/neierobezots-internets-aplikacijam. Accessed: 2021-08-25.

[170] Messaggio: Market Overview Latvia. https://messaggio.com/messaging/latvia/. Accessed: 2021-08-25.

[171] Tele2 (Lithuania). https://tele2.lt/. Accessed: 2021-08-25.

[172] Telia (Lithuania). https://www.telia.lt/. Accessed: 2021-08-25.

[173] Bite (Lithuania). https://www.bite.lt/. Accessed: 2021-08-25.

[174] Nemokamos paslaugos. https://www.bite.lt/planai. Accessed: 2021-08-25.

[175] Messaggio: Market Overview Lithuania. https://messaggio.com/messaging/lithuania/. Accessed: 2021-08-25.

[176] Tele2: Pildyk. https://tele2.lt/privatiems/aksesuarai/pildyk-pakuotes. Accessed: 2021-08-25.

[177] Pildyk Zero-Rating Plans. https://pildyk.lt/en/plans. Accessed: 2021-08-25.

[178] Telia: Ežys. https://www.teliacompany.com/en/about-the-company/markets-and-brands/lithuania/. Accessed: 2021-08-25.

[179] Ežys Zero-Rating Plans. https://www.ezys.lt/en/plans. Accessed: 2021-08-25.

[180] Tango (Luxembourg). https://www.tango.lu/en. Accessed: 2021-08-25.

[181] Tango Infinity. https://www.tango.lu/en/residential/offers/mobiles/subscriptions/tango-infinity. Accessed: 2021-08-25.

[182] POST (Luxembourg). https://www.post.lu/. Accessed: 2021-08-25.

[183] Streaming and Social. https://www.post.lu/particuliers/mobile/scoubido-avec-telephone#/bundles. Accessed: 2021-08-25.

[184] Orange (Luxembourg). https://www.orange.lu/en. Accessed: 2021-08-25.

[185] Luxembourg Online (Luxembourg). https://www.internet.lu/de/index.html. Accessed: 2021-08-25.

[186] Messaggio: Market Overview Luxembourg. https://messaggio.com/messaging/luxembourg/. Accessed: 2021-08-25.

[187] epic (Malta). https://epic.com.mt/. Accessed: 2021-08-25.

[188] GO (Malta). http://www.go.com.mt/. Accessed: 2021-08-25.

[189] WildCard. https://www.go.com.mt/wildcard. Accessed: 2021-08-25.

[190] Melita (Malta). https://www.melita.com/. Accessed: 2021-08-25.

[191] Messaggio: Market Overview Malta. https://messaggio.com/messaging/malta/. Accessed: 2021-08-25.

[192] KPN (Netherlands). https://www.kpn.com/. Accessed: 2021-08-25.

[193] T-Mobile (Netherlands). https://www.t-mobile.nl/. Accessed: 2021-08-25.

[194] Datavrije Muziek. https://www.t-mobile.nl/datavrije-muziek. Accessed: 2021-08-25.

[195] Vodafone (Netherlands). https://www.vodafone.nl/abonnement/mobiel. Accessed: 2021-08-25.

[196] Messaggio: Market Overview Netherlands. https://messaggio.com/messaging/netherlands/. Accessed: 2021-08-25.

[197] ACM Telecommonitor Q3 2020. https://www.acm.nl/sites/default/files/documents/telecommonitor-derde-kwartaal-2020.pdf. Accessed: 2021-08-25.

[198] Play (Poland). https://www.play.pl/. Accessed: 2021-08-25.

[199] PLAY NOW. https://www.play.pl/oferta/przejdz-do-play/play-abonament/. Accessed: 2021-08-25.

[200] Orange (Poland). https://www.orange.pl/. Accessed: 2021-08-25.

[201] Orange Flex Pass. https://flex.orange.pl/en/. Accessed: 2021-08-25.

[202] Plus (Poland). http://www.plus.pl/. Accessed: 2021-08-25.

[203] Plus Darmowytransfer. https://www.plus.pl/telefon-na-karte. Accessed: 2021-08-25.

[204] T-Mobile Supernet Video. https://www.t-mobile.pl/c/supernet-video. Accessed: 2021-08-25.

[205] Messaggio: Market Overview Poland. https://messaggio.com/messaging/poland/. Accessed: 2021-08-25.

[206] Statista: Mobile Operators in Poland. https://www.statista.com/statistics/1025450/poland-mobile-operators-in-terms-of-number-of-users/. Accessed: 2021-08-25.

[207] MEO (Portugal). https://www.meo.pt/. Accessed: 2021-08-25.

[208] Smart Net. https://www.meo.pt/internet/internet-movel/telemovel/pacotes-com-telemovel. Accessed: 2021-08-25.

[209] Vodafone (Portugal). https://www.vodafone.pt/. Accessed: 2021-08-25.

[210] Vodafone Pass. https://www.vodafone.pt/ajuda/artigos/tarifarios-roaming/vodafone-pass/o-que-sao-os-vodafone-pass-e-que-apps-incluem.html. Accessed: 2021-08-25.

[211] NOS (Portugal). https://www.nos.pt/. Accessed: 2021-08-25.

[212] WTF. https://www.nos.pt/particulares/pacotes/todos-os-pacotes/Paginas/wtf.aspx. Accessed: 2021-08-25.

[213] Messaggio: Market Overview Portugal. https://messaggio.com/messaging/portugal/. Accessed: 2021-08-25.

[214] Orange (Romania). https://www.orange.ro/. Accessed: 2021-08-25.

[215] Romania Abonamente Fun. https://www.orange.ro/abonamente/. Accessed: 2021-08-25.

[216] Vodafone (Romania). https://www.vodafone.ro/. Accessed: 2021-08-25.

[217] Vodafone Pass. https://www.vodafone.ro/pass. Accessed: 2021-08-25.

[218] Telekom (Romania). https://www.telekom.ro/. Accessed: 2021-08-25.

[219] Oferta Promoţională Messaging. https://media.telekom.ro/images/docs/Legal_docs/Mobile/Conditii_generale_de_acces_al_furnizorilor_in_Oferta_Promotionala_Messaging_in_vigoare_de_la_data_de_06_04_2017_TKRM.pdf. Accessed: 2021-08-25.

[220] Digi (Romania). https://www.digi.ro/. Accessed: 2021-08-25.

[221] Messaggio: Market Overview Romania. https://messaggio.com/messaging/romania/. Accessed: 2021-08-25.

[222] Statista: Romania Main Mobile Service Provider. https://www.statista.com/statistics/1134383/romania-main-mobile-service-providers-by-market-share/. Accessed: 2021-08-25.

[223] Romanian Constitutional Court declares SIM Registration unconstitutional. https://edri.org/our-work/romania-mandatory-sim-registration-declared-unconstitutional-again/. Accessed: 2021-08-25.

[224] Orange (Slovakia). https://www.orange.sk/. Accessed: 2021-08-25.

[225] Orange Dátový balík nonstop. https://www.orange.sk/nonstop-datove-baliky. Accessed: 2021-08-25.

[226] Telekom (Slovakia). https://www.telekom.sk/. Accessed: 2021-08-25.

[227] Telekom StreamOn. https://www.telekom.sk/wiki/ostatne/streamon. Accessed: 2021-08-25.

[228] O2 (Slovakia). https://www.o2.sk/. Accessed: 2021-08-25.

[229] O2 SMART Paušál. https://www.o2.sk/aplikacie-pre-o2-smart-pausal. Accessed: 2021-08-25.

[230] 4ka (Slovakia). https://www.4ka.sk/. Accessed: 2021-08-25.

[231] Messaggio: Market Overview Slovakia. https://messaggio.com/messaging/slovakia/. Accessed: 2021-08-25.

[232] Telekom (Slovenia). https://www.telekom.si/en. Accessed: 2021-08-25.

[233] A1 (Slovenia). https://www.a1.si/. Accessed: 2021-08-25.

[234] A1 Play. https://www.a1.si/play. Accessed: 2021-08-25.

[235] Telemach (Slovenia). https://telemach.si/. Accessed: 2021-08-25.

[236] T-2 (Slovenia). https://www.t-2.net/. Accessed: 2021-08-25.

[237] Messaggio: Market Overview Slovenia. https://messaggio.com/messaging/slovakia/. Accessed: 2021-08-25.

[238] Movistar (Spain). https://www.movistar.es/. Accessed: 2021-08-25.

[239] Orange (Spain). https://www.orange.es/. Accessed: 2021-08-25.

[240] Vodafone (Spain). https://www.vodafone.es/. Accessed: 2021-08-25.

[241] Vodafone Pass. https://www.vodafone.es/c/particulares/es/productos-y-servicios/movil/vodafone-pass/. Accessed: 2021-08-25.

[242] Yoigo (Spain). https://www.yoigo.com/. Accessed: 2021-08-25.

[243] Messaggio: Market Overview Spain. https://messaggio.com/messaging/spain/. Accessed: 2021-08-25.

[244] Statista: Mobile Phone Provider Market Share in Spain. https://www.statista.com/statistics/745319/mobile-phone-provider-market-share-in-spain/. Accessed: 2021-08-25.

[245] Telia (Sweden). https://www.telia.se/. Accessed: 2021-08-25.

[246] Telia Fri surf Sociala medier. https://www.telia.se/privat/telefoni/frisurfsocial. Accessed: 2021-08-25.

[247] Tele2 (Sweden). https://www.tele2.se/. Accessed: 2021-08-25.

[248] Tele2 Comhem Play. https://www.tele2.se/tv/comhemplay. Accessed: 2021-08-25.

[249] Telenor (Sweden). https://www.telenor.se/. Accessed: 2021-08-25.

[250] Telenor Stream. https://www.telenor.se/handla/tv/stream/. Accessed: 2021-08-25.

[251] Tre (Sweden). https://www.tre.se/. Accessed: 2021-08-25.

[252] Musikstreaming. https://www.tre.se/varfor-tre/hos-tre/musikstreaming. Accessed: 2021-08-25.

[253] Messaggio: Market Overview Sweden. https://messaggio.com/messaging/sweden/. Accessed: 2021-08-25.

[254] A1 SIMply S. https://www.a1.net/handys/neuer-vertrag/tarife-ohne-handy/s/sim-karte-ohne-bindung. Accessed: 2021-08-25.

[255] Magenta Mobile Youth SIMO S. https://www.magenta.at/handytarife/jugendtarif. Accessed: 2021-08-25.

[256] Drei Perfect SIM M. https://www.drei.at/de/shop/tarife/handytarife/sim-only-b/. Accessed: 2021-08-25.

[257] Telekom Simpa XS. https://www.simpa.hr/tarife. Accessed: 2021-08-25.

[258] A1 Spikalica. https://www.a1.hr/privatni/mobiteli/a1-na-bonove. Accessed: 2021-08-25.

[259] Vodafone Oferta Roaming 15. https://www.vodafone.ro/personal/servicii-si-tarife/cartela-vodafone/roaming/tarife-standard/. Accessed: 2021-08-25.

[260] Telekom Optiunea N5. https://www.telekom.ro/product/optiunea-n5/preplan148/. Accessed: 2021-08-25.

[261] Snapchat avatar. https://app.snapchat.com/web/deeplink/snapcode?username=michelleobama&type=SVG&size=240. Accessed: 2021-09-29.

[262] Whatsapp Web JavaScript File. https://web.whatsapp.com/vendor1~bootstrap_qr.2964a84e720ddeb3b0e5.js. Accessed: 2021-09-29.

[263] Twitter Communication with WhatsApp Support. https://twitter.com/GGegenhuber/status/1423358534461362184. Accessed: 2021-09-29.

[264] FM4 App stream. https://orf-live-fm4.mdn.ors.at/. Accessed: 2021-09-29.

[265] FM4 Website stream. https://orf-live.ors-shoutcast.at/. Accessed: 2021-09-29.

[266] Facebook Messenger Endpoint. https://graph.facebook.com. Accessed: 2021-09-29.

[267] Facebook Messenger Endpoint. https://b-graph.facebook.com. Accessed: 2021-09-29.

[268] Facebook Messenger Endpoint. https://z-m-graph.facebook.com. Accessed: 2021-09-29.

[269] Facebook Messenger Endpoint. https://lookaside.facebook.com. Accessed: 2021-09-29.

[270] Facebook Messenger Endpoint. https://scontent.xx.fbcdn.net. Accessed: 2021-09-29.

[271] Facebook Messenger Endpoint. https://www.messenger.com. Accessed: 2021-09-29.

[272] Facebook Messenger Endpoint. https://scontent-vie1-1.xx.fbcdn.net. Accessed: 2021-09-29.

[273] Facebook Messenger Endpoint. https://video-vie1-1.xx.fbcdn.net. Accessed: 2021-09-29.

[274] Facebook resource. http://static.xx.fbcdn.net/rsrc.php/v3/yb/r/esSUX1iWbDo.png. Accessed: 2021-09-29.

[275] Creative Commons Attribution-ShareAlike 3.0 Unported (CC BY-SA 3.0). https://creativecommons.org/licenses/by-sa/3.0/deed.en. Accessed: 2021-10-10.