ORANGE TRANSPARENCY REPORT ON FREEDOM OF EXPRESSION AND PROTECTING PRIVACY

2017 data

Orange is one of the leading telecommunications carriers in the world, with a turnover of €41.1 billion in 2017 and 151,600 employees at 31 December 2017, 96,000 of which are in France. Operating in 29 countries, the Group had a total of 273 million customers worldwide at 31 December 2017, including 46 million 4G customers and 4.7 million high-speed internet customers. Orange is also one of the world leaders in providing telecommunication carrier services to multinational companies under the Orange Business Services brand.

Our commitment to freedom of expression and confidentiality

As a telecommunications carrier, Orange strives to ensure that human rights are respected, particularly regarding the use of Information and Communication Technology (ICT). Freedom of expression and the protection of privacy are topics that have a particularly significant effect on the telecommunications sector. This is a key reason for our participation in the Global Network Initiative (GNI). In March 2017, Orange and a number of carriers and device manufacturers from the sector-based group Telecom Industry Dialogue (TID) joined the GNI (https://globalnetworkinitiative.org/), of which Orange is currently a member of the Board of Directors. This multi-stakeholder platform, which includes internet carriers, telecommunications carriers, device manufacturers, NGOs, academics and socially responsible investors, focuses on issues of freedom of expression and protection of privacy in response to government requests. Following the admission of the TID's members to the GNI, the guiding principles of the GNI were updated (https://globalnetworkinitiative.org/gin_tnetnoc/uploads/2018/04/GNI-Principles-on-Freedom-of-Expression-and-Privacy.pdf). These principles form a reference framework for drafting and implementing policies and processes within the Group in terms of freedom of

expression and protection of privacy in the ICT sector. Every year, Orange issues a report on the measures put in place to guarantee these principles. From 2019, i.e. for data from 2018, this self-assessment report will be more formal, and in particular will be reviewed by our CSR auditors, who will hold GNI certification for this type of assessment. In accordance with the GNI's processes, this audit – which specifically covers the implementation of the GNI's principles on freedom of expression and privacy – will take place every two years in addition to our own CSR reporting process, which is audited annually.

The GNI is a multi-stakeholder platform that speaks with one voice and that holds dialogues with governments and international institutions (the United Nations, the European Commission and the Council of Europe) to make recommendations regarding local policies or laws to ensure that freedom of expression and privacy are protected around the world. In 2017, we made contributions on the topic of government-requested network shutdowns, which are becoming increasingly frequent, and on regulation of online content, including hateful content, extremist content, and fake news.

Like all telecommunications carriers, Orange must obey government orders in accordance with national security and legal requirements. This is a universal obligation that forms part of the laws and regulations of each country as well as of the terms of telecommunications carriers' licences worldwide.

In addition, governments around the world should publish transparency reports regarding freedom of expression and protection of privacy in order to provide full and comprehensive transparency. Some countries already publish reports on these topics, but this is not common practice. To overcome this inertia, Orange has committed to regularly publishing information on government requests to the extent permitted by local legislation. This ensures transparency in terms of monitoring human rights-related government requests, particularly those related to the ICT sector.

For the fourth year running, Orange is publishing a report on government requests related to freedom of expression and protection of privacy. This document reinforces the public commitment made by Orange when it signed a charter on the protection of personal data and privacy in 2013.

The indicators included in this report

To report on action taken by governments regarding freedom of expression and protection of privacy, we have chosen two indicators:

- government requests for **interceptions**
- government requests for **customer data**

To facilitate comparison between the many reports in existence in the industries in question, we have decided to choose the most commonly used indicators.
The 'interceptions' and 'customer data' indicators refer to the number of government requests made to Orange. A single request may relate to many customers, and one customer may be the subject of successive requests over the course of the year.

Requests can differ between issuing authorities and countries. In order for Orange to carry out these requests, they must meet three formal requirements:

- the authority making the request must have jurisdiction to do so
- the request must be made via formal channels
- the request must comply with the country's laws and regulations

After these elements have been verified, the request is carried out, rejected or referred back to the requesting party to obtain the missing information needed to assess the request.

a) Interceptions

This indicator represents the number of requests from governments or from other public authorities, such as requisition orders and administrative requests requiring the content of telephone communications to be disclosed.[1].

The ETSI (European Telecommunication Standardization Institute) has set out an international standard defining interception as "legally sanctioned official access to private communications".
This standard specifies that:

- Information on how interception measures are implemented in a given telecommunications installation must not be disclosed to unauthorised persons.
- Information on the techniques used to target the identities and services that are the subjects of the interception must not be disclosed to unauthorised persons.
- Only the overall figure is published, except if a managerial decision or national legislation prevents this. A managerial decision may be made based on the fourth GNI principle, which has been adopted by Orange: protecting our staff under all circumstances. Such a decision is taken by the CEO of the subsidiary or by the Group's executive management.

The table below does not show figures for some countries. In some cases, this is due to the policies and laws in place, while in other cases, the authorities may have direct access to the content of communications, regardless of the technique used. It may also be that no request was made to Orange.

b) Customer data

This indicator corresponds to the number of requests from a range of stakeholders, such as governments, judicial authorities, or the police, for a variety of data, including[2]:

- Call details (traffic data such as originator, recipient, frequency, duration, etc.)
- Customer identification data (surname, first name, address, date of birth, etc.)
- Geolocation (relays or GPS coordinates)
- Billing and payment data

This indicator also covers all types of communications made using landlines, broadband and mobile lines, regardless of the type of device used (landline handset, mobile phone, smartphone, TV, PC, tablet or smart device) or of the Orange package involved.

Interception and customer data requests - 2017

Country	Number of employees	Number of customers	Interceptions	Customer data
France[1]	92,025	75,420,221	8 758	52 254
Poland[2]	14,956	21,167,724	not published	not published
Spain	7202	24,190,649	54,852	52,805
Belgium	1635	4,097,068	34,485	
Romania	3440.5	9,910,033	not published	not published
Slovakia	1136	3,011,377	not published	18,387
Moldova	1154	2,221,100	not published	not published
Morocco	1136	15,223,583	not published	not published
Senegal	1829	8,749,263	0	22,011
Mali	616	12,527,664	0	9510
Côte d'Ivoire	1428	14,398,062	0	3253
Egypt	4089	34,461,249	not published	not published
Niger	420	1,869,003	13	3357
Jordan	1763	3,538,905	-	15,014
Madagascar	869	1,978,111	2092	
Botswana	370	940,035	-	350
Cameroon	603	7,244,937	-	27,312
Guinea	368	6,784,674	-	3173
DRC	1437	9,059,172	26	981
Tunisia[3]	1200	4,000,000	20,069	5795

[1] In the case of France, the data presented refers only to requests made by the intelligence services, and is taken from the annual report of the National Commission for the Control of Intelligence Techniques (CNCTR). In this respect, they concern interceptions, access to connection data in deferred time and geolocations, not to Orange, but to all operators in France. Geolocation requests are presented gross of any refusals

[2] This information is usually published by the Polish authorities in an official report. Reports for 2016 & 2017 have yet to be published.

[3] The published figures regarding the number of customers and of employees in Tunisia are not included in the Group's published figures because of Tunisia's non-consolidation.

Major events related to freedom of expression

For a telecommunications carrier, major events are occasional government requests that affect a large number of customers at the same time. These events may be network shutdowns, such as internet or SMS shutdowns; shutdowns of services, such as of social media; or the mass sending of SMS messages (government information) and requests for information about all of our customers.

Orange's procedure for responding to these major events involves receiving a formal and traceable request, i.e. an order that is both written and signed by a public authority with the necessary jurisdiction and based on a law or regulation.

In addition, if the request is not made in compliance with these formalities, Orange reserves the right to alert the international community and supranational authorities.

In 2017, the Group experienced nine major events of this type, which represents the continuation of a significant increase on previous years, first observed in 2016. The growing number of requests in 2017 is primarily due to multiple requests for shutdowns made by certain governments in their countries.

Number of major events related to freedom of expression per year

Major events mean that it is impossible to publish details of these requests, such as the countries involved, dates, circumstances and reasons given. Publishing this information could expose our staff to risks in various Group countries.

This position is enshrined in principle 4 of the GNI, which recommends protecting the safety and freedom of all staff who may be placed in danger.

Content restriction requests

Orange's position in terms of content restriction is to obey the laws in force in the countries in which we operate. Orange obeys administrative and legal requests to remove illegal content. We act on government requests regarding specific cases. In most cases, the content restriction applied involves blocking a website or an IP address. As a telecommunications carrier, Orange does not examine Internet content and cannot block specific content, only domains.

Regulatory and legal frameworks

Regulations in this area vary by country and according to events.
As such, following on from the Telecom Industry Dialogue (TID), the GNI regularly publishes a review of the legal framework in a number of the countries in which its members operate. The study can be accessed at the following address: https://globalnetworkinitiative.org/?s=legal+framework

France: Regulations on the interception of communications and the obligation of telecommunications carriers to disclose customer data

The universally recognised principle of disclosure remains based on the fact that all requests must be made officially.

They may take a number of forms:
1. Requests from the judicial system: these come from legal decisions as a result of the application of various laws:
a. Code of Criminal Procedure
b. The Postal and Electronic Communications Code

2. Requests from a government body under the supervision of a judge or from an independent administrative authority (CNCTR or CNIL) in accordance with the Internal Security Code.