# ORANGE TRANSPARENCY REPORT
# ON FREEDOM OF EXPRESSION AND PRIVACY PROTECTION

## Year 2015

Orange, a founding member of the Telecommunications Industry Dialogue (TID), a group of telecommunications operators and vendors founded in 2011 to foster a joint dialogue with stakeholders on human rights, has committed to publishing an annual report on major human rights-related events.

Like all telecommunications operators, Orange must comply with government orders as defined by national security regulations and the law. This is a universal obligation which is laid out in each country's laws and regulations, as well as in licenses for telecommunications operations worldwide. For the second consecutive year, Orange is publishing a report on government requests related to freedom of expression and privacy protection. This publication backs up the public commitment that Orange made in 2013 when it signed a charter on its commitment to personal data and privacy protection.

## 1) Interceptions and data disclosures by country

We have selected two significant indicators to account for government actions related to freedom of expression and privacy protection. These indicators are also frequently used by other telecommunications operators and internet service providers.
Please note that each country can set its own unique rules: filtering by a public regulator may or may not be required, and different authorities, including ministries, the police, gendarmerie or courts, may be authorised to make requests - which entail different verification and inspection procedures. Certain countries, including France, also publish their own data.

For both the "interceptions" and "customer data" indicators, the number given is the number of requests received. The number of clients affected was not considered usable, given that a single request can involve multiple customers and that a single customer can be involved in a series of requests during the course of the year under the same name or slightly different ones, particularly in the case of legal entities.
These requests can take different forms depending on the authority making the request and the country in question. The minimum elements required for verification are: a formal request, the jurisdiction of the issuing authority, and the legal basis for the request. The group's procedure includes verifying that all requests are duly formalised; non-compliant requests are rejected or sent back for further information.

## a) Lawful interceptions

This is the number of requests made by governments or other public authorities, including requisition orders and subpoenas requiring the disclosure of the content of calls.

The ETSI (European Telecommunication Standardization Institute) has defined lawful interceptions as: "legally sanctioned official access to private communications."
The standard also specifies that:

- Information on how interception measures are implemented in a given telecommunications installation must not be made available to unauthorised persons.
- Information on the techniques used to target the identities and services which are the targets of the interception must not be made available to unauthorised persons.
- Only the overall figure is published, except where prohibited by an executive decision or the country's regulations. Executive management may refuse to publish the figure on the basis of the 5th principle of the TID, which we have adopted: always protect our personnel. The decision can be made by a subsidiary CEO or by Group-level executive management.

The table below does not show a figure for certain countries. This is due either to the reasons given above (national sovereignty and legal compliance) or, in certain cases which it is impossible to list precisely, the authorities already have direct access by one or more technical means.
It is also possible that Orange did not receive any requests.

## b) Customer data

This is the total number of government or judicial requests for a wide range of data:

- Call details (traffic data, including sender, destination, frequency, duration, etc.)
- Customer identification data (first and last names, address, date of birth, etc.)
- Geolocation (relays or GPS coordinates)
- Invoicing and payment information

The figure given is the total number of legal requests, regardless of the source (requesting agency). The figure consolidates all types of communications on fixed, broadband or mobile lines, regardless of the type of device used (fixed set, mobile, smartphone, TV, PC, tablet, or connected object) or the Orange offer involved.

## Requests for interceptions and customer data

| Country | Interceptions | Customer data |
|---|---|---|
| **Belgium** | 48572 | |
| **Poland** | Not published | Currently awaiting official report |
| **Spain** | 52445 | 36105 |
| **Slovakia** | Not published | 47993 |
| **Romania** | Not published | Not published |
| **Moldova** | Not published | Not published |
| **France** | Currently awaiting official report | Currently awaiting official report |
| **Botswana** | 0 | 340 |
| **Jordan** | Not published | 720 |
| **Egypt** | Not published | Not published |
| **Senegal** | 0 | 13577 |
| **Côte d'Ivoire** | 0 | 3500 |
| **Mali** | 0 | 8025 |
| **Niger** | 0 | 2084 |
| **Cameroon** | 0 | 17091 |
| **DR of Congo** | 0 | 385 |
| **Guinea (Conakry)** | 0 | 2017 |
| **Tunisia** | 0 | 1800 |
| | | |

## 2) Major events related to freedom of expression

For telecommunications operators, the major events in this area are occasional government requests which simultaneously affect large numbers of customers: cutting access to networks (internet, SMS, etc.) or services (social media), sending out propaganda via mass SMS, requests for information on all of its customers, etc.
Orange's general procedure in these cases is to require a traceable request, i.e. a written order grounded in the law and signed by the competent authority. Orange reserves the right to alert the international community and supra-national authorities in the event of non-compliance with local legislation.

In 2015, the Group recorded three major events of this type (network or service cuts).
Due to the potential risk to employees in certain Group countries, it is currently impossible to disclose the countries and dates where these events occurred (compliance with principle 5 of the TID). For similar reasons, we cannot publish the details on these cuts, such as the circumstances and justification provided.

## 3) Regulatory and legal frameworks

The regulations in this area vary both by country and over time, as the situation changes. The Telecom Industry Dialogue (TID) regularly publishes a review of the legal framework in a number of the countries where its members operate. The study is available at (http://www.telecomindustrydialogue.org/). The legal and regulatory framework was modified in 2015 in many of the countries where the Group operates, often as part of anti-terrorist efforts. France is one of the Group countries which has seen the most significant changes.

**France: Regulations on the interception of telecommunications and the legal obligation of telecommunications operators to disclose customer data**

The universally recognised principle of disclosure is based on the fact that all requests must be made through the legal system.

They can take a number of different forms:

1. Orders issued directly by judicial bodies: these are court orders in application of various legislation:
    a. the penal procedure code
    b. the postal services and electronic communications code

    c. Orders from government agencies under the supervision of a judge or an independent administrative body (CNCTR or CNIL), in application of the code of homeland security

2. European Regulations (upcoming directive on data)