Ofcom
making communications work
for everyone

The provision of Calling Line Identification facilities and other related services over Electronic Communications Networks

DRAFT GUIDELINES:

Publication Date: 19 September 2017

About this document

Calling Line Identification (CLI) provides information to the recipient of a call about the party making a telephone call. CLI data is also used in regulatory and enforcement action, for example, to identify the sources of nuisance calls. CLI data needs to be provided correctly and delivered across networks accurately. As individuals have the right to withhold their CLI to maintain their privacy, it is also important that any information associated with the CLI is passed on reliably so that the privacy of individuals can be respected.

General Condition GC C6 requires CPs to provide CLI facilities, unless they can demonstrate that it is not technically feasible or economically viable to do so. In doing so, the CLI that is provided must include a valid, dialable telephone number which uniquely identifies the caller. This document sets out guidelines on how CLI data should be carried through different networks and the responsibilities of different parties involved in the routing of a call. Its aim is to improve the consistency of CLI data presented to consumers, whilst also complying with statutory requirements on the privacy rights of individuals making and receiving calls.

Contents

Section

Annex

1. Summary

1.1 Calling Line Identification (CLI) provides information about the party making a telephone call. CLI data consists of the caller's line identity along with a privacy marking, which indicates whether the number can be shared with the recipient of the call. For this to work reliably, it requires that the CLI data is provided correctly and that this information is passed between networks accurately. As the CLI identifies the end user associated with that number, privacy choices of the end user need to be respected.

1.2 The CLI data that is presented with a call can provide assurance to the recipient of the call about who they are talking to. However, the passage of CLI information is vulnerable to misuse, for example the insertion of false information to intentionally mislead the recipient of the call of the identity of the caller.

1.3 There needs to be a consistent approach to the handling of CLI data, from call origination through to call termination, particularly for calls that pass through two or more network providers. This is to ensure that the CLI itself can be passed on accurately and that the privacy choices made by end users about their CLI data are respected by all communications providers involved in the origination, transmission and termination of that call.

1.4 Ofcom's General Conditions require CPs to provide CLI facilities, where technically feasible and economically viable. They also require CPs to ensure that any CLI data provided with and/or associated with a call includes a valid, dialable telephone number which uniquely identifies the caller. The aim of this document is to establish the principles for this approach, setting out what is expected of CPs to meet these requirements and to guide all communications providers that participate in the origination, transmission and termination of a call in the UK.

2. Background, Legal Context and Scope

Background

2.1 This document sets out the approach to the handling of caller information from the initiation of a call to its termination. The aim of this document is to ensure that the accuracy of CLI data is protected throughout the transmission of a call and that the privacy choices of end users are respected and maintained throughout all parts of the call process, from the origination, to the transmission and to the termination of a call.

2.2 A common approach across CPs is necessary as this will give CPs and end users certainty about the information that is provided with a telephone call. This is because the end-to-end conveyance of a call originated by an end user frequently requires the collaboration of several network providers and it is important that CPs treat CLI data in the same way. This document replaces the previous version of the guidelines which were originally published in 2003 and subsequently amended in 2007.

Legal Context

2.3 The rules for the display of CLI data is set out in the General Conditions of Entitlement, in GC C6.[1] This requires CPs, subject to technical feasibility and economic viability, to provide Calling Line Identification facilities. It also specifies that the CP must ensure that any CLI data provided with a call includes a valid, dialable telephone number which uniquely identifies the caller. Where CPs identify a call that has invalid or non-dialable CLI data the GC requires the CP to prevent these calls from being connected to the called party, where technically feasible.

2.4 The CLI is personal data, within the meaning of relevant data protection legislation. Therefore, CPs must also comply with Regulations 10 – 13 of the Privacy and Electronic Communications (EC Directive) Regulations (PECR) 2003.[2] This sets out a fundamental series of privacy rights for end users making and receiving calls.

2.5 PECR was amended in 2016 to require those making calls for direct marketing purposes to not prevent the presentation of the calling line on a called line and that the CLI presents the identity of a line on which the caller can be contacted.[3]

2.6 We may need to make changes to these guidelines from time to time. We will consult on these changes in the usual way when appropriate.

[1] https://www.ofcom.org.uk/__data/assets/pdf_file/0023/106394/Annex-14-Revised-clean-conditions.pdf
[2] http://www.legislation.gov.uk/uksi/2003/2426/contents/made
[3] http://www.legislation.gov.uk/uksi/2016/524/pdfs/uksi_20160524_en.pdf

Scope

2.7 The current guidelines would apply to CPs who fall under the scope of the requirements of GC C6 and of PECR. Therefore this would apply to all providers of Publicly Available Telephone Services and Public Electronic Communications Networks over which Publicly Available Telephone Services are provided.

2.8 Although CPs are required to comply with the General Conditions for CLI, CPs must be mindful of the privacy requirements relating to the Connected Line[4], arising from PECR. Therefore, we would also expect CPs to follow these principles for Connected Line (COL) information. However, unlike CLI, this is not mandated under our General Conditions.

2.9 We would expect interconnect agreements between CPs within the scope of these requirements to reference these Guidelines with a requirement that the contracting parties abide by them.

Technical Standards

2.10 The format of telephone numbers is defined by the ITU in their International Public Telecommunication Numbering Plan.[5] This document sets out the structure of telephone numbers and how the numbers should be interpreted.

2.11 In the UK, CPs have developed the rules that must be applied when an interconnection is made between different CPs, via the NICC[6]. These rules are set out in ND1016.[7] CPs interconnecting with other CPs should follow these rules, although there may be instances where there may be reasons why it is not possible to adhere to them.

Enforcement

2.12 Although these guidelines are not binding, we may take them into account in our enforcement actions when considering compliance against other requirements. These include:

- the General Conditions, requiring CPs to provide CLI facilities, including CLI Data with a telephone number that is valid, dialable and uniquely identifies the caller; and
- the Communications Act 2003, which gives Ofcom powers to take enforcement action where there are grounds for believing there is persistent misuse of an Electronic Communications Network or Electronic Communications Service. These powers may be exercised where end users knowingly cause unauthentic or misleading CLI data to be sent.[8]

[4] The Connected Line Identity (COL) represents the information about the called party.

[5] ITU-T Recommendation E.164 https://www.itu.int/rec/T-REC-E.164/en

[6] NICC is the UK telecoms industry standards forum that develops interoperability standards for UK communications networks.

[7] http://www.niccstandards.org.uk/files/current/ND1016v3%202%201.pdf?type=pdf

[8] https://www.ofcom.org.uk/consultations-and-statements/category-1/review-of-how-we-use-persistent-misuse-powers

2.13 The Information Commissioner’s Office has primary responsibility for enforcement against the requirements of PECR.

3. End Users' Privacy Rights

3.1 This section sets out the principles that arise from the Privacy and Electronic Communications (EC Directive) Regulations (PECR) 2003[9], in particular regulations 10 to 13, which set out a series of fundamental privacy rights for end users making and receiving calls.

3.2 The rights of the calling party are that:

a) They must be able, using a simple means and free of charge, to prevent the display of their number at the point where their call terminates – this option may be exercised by users on a call-by-call basis and by subscribers on a more permanent basis by preventing the display of CLI data on all calls made from a particular line;

b) But that any person making calls for direct marketing purposes must not withhold their number (see below).

3.3 The rights of the called party are that:

a) They must be able, using a simple means and free of charge for reasonable use, to prevent the display of CLI data relating to incoming calls (so that help-lines are able to offer an assurance of anonymity to people who call them).

b) Where CLI data is displayed before a call is established, they must be able, using a simple means and free of charge, to reject calls where the caller has (i) been given the option of preventing the display of their CLI data and (ii) deliberately chosen to exercise this option. The service is commonly known as Anonymous Call Reject (ACR).

c) Where connected line identification (COL) is in use they must be able, using a simple means and free of charge, to prevent the display to the caller of the actual number to which an incoming call has been connected.

3.4 The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2016[10] introduced new requirements specifically in relation to direct marketing calls and calls on automated calling systems. The amended regulations 19 and 21 of PECR stipulate that any person making direct marketing calls or calls on automated calling systems must not prevent the presentation of the identity of the calling line on the called line and must present the identity of a telephone number on which they can be contacted.

3.5 An additional right that arises from the application of general data protection principles is the ability of called end users to render received CLI data that is stored by a Communications Provider in a form directly retrievable by an end user inaccessible. This capability is commonly known as call return/1471 erasure.

3.6 Where a called end user has selected to use Anonymous Call Reject, in accordance with paragraph 3.3(c), the calling end user should be advised as to why the call has been

[9] http://www.legislation.gov.uk/uksi/2003/2426/contents/made

[10] http://www.legislation.gov.uk/uksi/2016/524/pdfs/uksi_20160524_en.pdf

rejected, for example a recorded announcement with an explanation that the call was rejected because they restricted their CLI.

Exceptions to the caller's privacy rights

3.7 PECR also sets out exceptions where the caller's right to prevent the display of their CLI data can be overridden. These are for calls that are made to the emergency services or to assist relevant authorities in investigating and tracing malicious or nuisance calls.

3.8 Privacy rights may also be restricted in order to safeguard national security, defence, public security and to facilitate the prevention, investigation, detection and prosecution of criminal offences. The Investigatory Powers Act 2016 creates a legal framework within which Communications Data, which includes CLI data, may be obtained and disclosed to designated authorities in order to secure these objectives.

4. Requirements for Communications Providers providing CLI facilities

4.1 This section sets out the principles for Communications Providers providing Calling Line Identification facilities about how CLI data must be provided and passed through their networks to meet the requirements in the General Conditions and respect end users' privacy wishes.

4.2 General Condition C6 requires Regulated Providers to provide CLI facilities and enable them by default unless they can demonstrate that it is not technically feasible or economically viable to do so. This must be provided at no additional or separate fee. The regulated provider must inform subscribers if CLI facilities are not available on the service they are providing. We expect CPs to inform their customers at the start of their contract whether they are able to provide the functions of the CLI facilities and to update their customers where the situation changes.

4.3 GC C6 also specifies that when providing CLI facilities, the Regulated Provider must ensure, so far as technically feasible, that any CLI data provided with and/or associated with a call includes a valid, dialable telephone number which uniquely identifies the caller and that it respects the privacy choices of end users. Where technically feasible, the Regulated Provider must take all reasonable steps to identify calls which have invalid or non-dialable CLI data and prevent those calls from being connected to the called party.

4.4 The CLI facilities are the functions supporting the provision of CLI data with a telephone call. The CLI data consists of a telephone number and an associated privacy marking. This represents the identity of the party making the call.

4.5 These rules help to ensure that the correct information is made available to end users, where appropriate, and for network functions, such as call tracing. Where a CP is unable to provide CLI facilities to their customer, they should inform their customer.

4.6 In addition to these principles, this section also sets out where CPs must not have access to their customer's CLI data, to comply with data privacy rules.

Principles for the provision and handling of CLI data

4.7 The fundamental principles behind the provision of CLI facilities are those of validity, privacy and integrity. As CPs will need to co-ordinate between different networks to follow these principles, we recommend that CPs refer to industry standards, such as NICC's ND1016.

Validity

4.8 The General Conditions require that CPs must present a valid, dialable telephone phone which uniquely identifies the caller. This responsibility to ensure that CLI data fulfils these requirements falls to all CPs involved in the interconnection of the call.

4.9 It is the responsibility of the originating CP to ensure that the correct CLI data is generated at call origination. They are responsible for either providing the CLI from a number range that has been allocated to them or seeking assurance from the customer that they are using a CLI that they have permission to use (either because they have been directly allocated that number or have been given permission by a third party who has been allocated that number). For calls generated on networks where these requirements do not apply e.g. international calls, this responsibility falls on the CP at the first point of ingress to the UK networks. Where the CP at the ingress does not reasonably trust the CLI data that is being provided, or where CLI data is not available, the CP should insert a CLI from a range that has been allocated to them for this purpose. The CLI provided should also route to a non-chargeable explanatory announcement, in case the CLI is displayed to an end user.

4.10 Transit CPs should also ensure that the CLI data that they pass with a call contains valid CLI. The terminating CP should present only valid CLI data to the end user. The CLI presented could be a Network Number or a Presentation Number. The Presentation Number is not always required, but the call should always be associated with a Network Number, as a minimum. The requirements for these numbers are explained in more detail in Annex 1.

4.11 The CLI presented must be a number which fulfils the technical requirements as specified in ND1016, and the following requirements:

- It must be a valid number - This is a number that complies with the ITU-T numbering plan E.164.[11] It must also be a number that has been allocated for use in the UK in the National Telephone Numbering Plan.[12]
- It must be a dialable number, i.e. a number that is in service. This number must be one that identifies the caller (which can be an individual or an organisation)[13] and can be used to make a return or subsequent call;
- It must uniquely identify the caller, i.e. be a number that the user has been given authority to use (either because it is a number that has been allocated to them or because the user has been given permission from a third party who has been allocated that number)[14]; and
- It must not be a number that results in charges in excess of the cost of calling a standard geographic number or a mobile number.

4.12 In addition to ensuring that CLI data is populated properly, the General Conditions also place an obligation on all CPs to prevent calls that have invalid or non-dialable CLIs from reaching the called party. This means that CPs who have the technical capability should block or divert the calls. For the originating CP, this means they should not initiate calls that have invalid or non-dialable CLIs. Transit and terminating CPs should stop these calls.

[11] ITU-T Recommendation E.164 (11/2010) "The international public telecommunication numbering plan" https://www.itu.int/rec/T-REC-E.164/en

[12] https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/numbering

[13] In the case of a Network Number, for a call from a fixed location this should represent the fixed ingress point of that call. Any Presentation Number used should always represent the identity of the caller. See Annex 1 for further details.

[14] This may be, for example, in the form of a contractual confirmation from the party who has been allocated that number.

4.13 Stopping a call can be either through blocking or filtering calls. Blocking is where the CP, subject to their technical capability, identifies calls with invalid or non-dialable CLI and prevents these calls from being connected to the end user. Alternatively, CPs could provide a call filtering service, where calls with invalid or non-dialable CLI are diverted to a mailbox, so that these calls are not immediately connected to the end user.

Privacy

4.14 To satisfy the end user's right to prevent the display of their number, the originating provider must provide the correct privacy marking alongside the number. This marking must indicate that the CLI is:

- Available – where the caller has been given the possibility of preventing the display of CLI data and has chosen not to do so
- Withheld - where the caller has been given the possibility of preventing the display of CLI data and has chosen to exercise this option
- Unavailable – In situations other than the above or when the accuracy of the classification is in doubt, for example where it is not possible to offer an end user privacy choices and ensure they are respected, where the display of the CLI data is prevented by CPs in order to preserve the anonymity of a caller's Network Number when a Presentation Number is available.

4.15 For calls received from a network outside the scope of these requirements, the CP at the first point of ingress to the UK networks is responsible for ensuring that the caller's privacy rights are respected. The CP receiving the call at the ingress to UK networks can use the same privacy markings as above, but in this context the markings have a different meaning:

- Available – where the CLI data is deemed to be reliable and the caller has chosen not to prevent the display of their CLI
- Withheld – where there is an explicit indication that the caller does not wish to make their CLI available to the recipient of the call
- Unavailable – where there is explicit indication that the originating the network has restricted the CLI on behalf of the calling party and their CLI should not be made available, or when the ingress CP has inserted a Network Number into the call as it has deemed the CLI data presented with the call unreliable

4.16 It is the responsibility of the CP terminating the call to ensure that CLI data is only displayed to the end user where the caller has chosen to make this information available and the recipient of the call has chosen not to prevent the display of CLI data relating to incoming calls.[15] For calls that are being passed to networks where these requirements do not apply, the CP at the point of egress should only pass on the CLI data where the caller has chosen to make this information available and where they have good reason to believe that the CPs in the onward chain will respect the privacy markings. Otherwise, to avoid a caller's identity being displayed to the called party, the CLI information should be deleted

[15] For COL, the originating CP (that is the originating CP for the party initiating the call) is responsible for ensuring that COL data is only presented where the called party has chosen to make this information available.

at the gateway exchange if the CLI information has been classified as 'withheld' or 'unavailable'.

Integrity

4.17 All CPs involved in the transmission of a call should do all that is technically feasible to ensure that the authenticity of the CLI data is maintained from call origination to call termination. Where this includes a Presentation Number, CPs must consider whether this number is sufficiently authentic and if further verification is required, subject to technical feasibility. Annex 1 sets out some of these scenarios.

Use of end user's CLI data within the network

4.18 Although PECR sets out the specific rules for CPs to help end users manage information relating to their privacy, CPs must also be mindful of the access they have to the end users' CLI data. They should only use their privileged access to this information where its use is essential to the provision of an Electronic Communications Service.

4.19 Therefore, this access should be limited to those staff for whom it is essential, for example for network and/or account management purposes and, in co-operation with the relevant authorities, for emergency calls and the tracing of malicious calls and similar activities.

4.20 CPs must respect the privacy of callers who have elected to prevent the display of their line identities by not exploiting this information for telemarketing or any commercial purpose other than billing and repair.

4.21 Furthermore, CPs must ensure that where callers have chosen to prevent the display of their line identities, the Network Number and Presentation Number should not be passed on to a party who is not a CP.

A1. A guide to Network and Presentation Numbers

Introduction

A1.1 Section 4 of this document sets out the guidelines relating to the CLI that is displayed to the end user. The CLI that is displayed can be either a Network Number or a Presentation Number representing the origin of the call. Every call must be associated with a Network Number. For the COL, the number that is displayed represents the destination of the call.

A1.2 The Network Number is a line identity that comprises a unique E.164 number (or from which that number may be reconstructed) that unambiguously identifies the line identity of:

- The fixed access ingress to, or egress from, a Public Telephone Network, i.e. the Network Termination Point (NTP);
- A Subscriber or terminal/telephone that has non-fixed access to a Public Telephone Network, i.e. the line identity that has been allocated to an individual subscription or terminal/telephone with a non-fixed access to the public network; or
- The first known UK PECN (or a node within that PECN) in the call path. This should only be used where the first known UK PECN does not reasonably trust the CLI data that is being provided or the CLI data is not available. In these circumstances, the privacy marking provided alongside the CLI should be marked as ‘unavailable’.
- The number that is used must not be a number that results in charges in excess of the cost of calling a standard geographic number or a mobile number.

A1.3 The authenticity of a Network Number is guaranteed as the number must be one which has been provided by the originating network and it is a number that has been allocated to the originating network provider.[16]

A1.4 The Presentation Number is a number nominated or provided by the caller that can identify that caller or be used to make a return or subsequent call. In the UK, the industry has recognised a number of scenarios where Presentation Numbers may be provided, as a commercial service, to meet differing customer calling requirements.

A1.5 Unlike a Network Number, a Presentation Number will not necessarily identify a call’s point of ingress to a public network. However, it may carry other useful information. The requirements of a Presentation Number are that:

- It must be a valid number, that complies with the ITU-T numbering plan E.164.
- It must be a dialable number that identifies the caller and can be used to make a return or subsequent call.

[16] The Network Number is used by the emergency services to ascertain the origin of an emergency call, hence should be representative of the PECN.

- It must be a number that the user has been given authority to use (either because it is a number that has been allocated to the user or because the user has been given permission from a third party who has been allocated that number); and
- It must not be a number that results charges in excess of the cost of calling a standard geographic number or a mobile number. (NB the exploitation of a Presentation Number to generate revenue-sharing calls may constitute persistent misuse of an Electronic Communications Network or Electronic Communications Service).

A1.6 In order to maintain the integrity of the CLI data as it is passed between networks, CPs must consider whether the Presentation Number is sufficiently authentic and if further verification may be required. Where additional verification is needed to demonstrate that the caller has permission to use the number, this could be in the form of a contract between the caller and the third party who has been allocated that number. A number of different types of Presentation Number services have been developed to meet these end user requirements and the following section lists the conditions that should be observed for their use.

Types of Presentation Number

Type 1

A1.7 A Presentation Number generated by the subscriber's network provider. The number is stored in the network and applied to an outgoing call at the local exchange by the provider. Because the number is applied by network equipment there is no need for it to be verified each time a call is made – instead the level of authenticity will depend on the checks made by a network provider that a subscriber is entitled to use a particular Presentation Number.

Type 2

A1.8 A Presentation Number which identifies a caller's extension number behind a DDI switchboard. Although the number or partial number is generated by the user's own equipment, the network provider is able to check that it falls within the range and length allocated to a particular subscriber. In this way the authenticity of the number may be ensured. It should be noted that some network providers classify Type 2 Presentation Numbers as network numbers (especially where the full number is constituted at the local exchange). This type of number is considered to carry sufficient authenticity to be classified as a network number and is carried as such by some networks.

Type 3

A1.9 A Presentation Number limited to the far-end break out scenario where a call's ingress to the public network may be geographically remote from where it was originated. The number is generated by the user's equipment and is not capable of being subjected to network verification procedures. Verification is based on a contract between the subscriber and the network provider in which the subscriber gives an undertaking that only authentic calling party numbers will be generated.

Type 4

A1.10 A Presentation Number available for the onward transmission of the originating number where a call breaks into a private network and breaks out again before termination, as in a DISA scenario. On the break out leg the number is generated by the user's equipment although it will have already been verified in consequence of having been delivered to the private network. To maintain the verification it is necessary to ensure that the number submitted by the private network is the number that was received.

A1.11 Network providers wishing to offer a Type 4 service will require a contractual commitment from customers that they will only submit CLIs that have been received from the public network. Unlike other types of Presentation Numbers, Type 4 numbers may not always be dialable: This will depend on the nature of the number received from the public network.

Type 5

A1.12 Presentation numbers that identify separate groups of callers behind a private network switch wishing to send different outgoing CLIs. A typical scenario is a call centre making calls on behalf of more than one client. Type 5 Presentation Numbers are generated by the user's equipment. Subscribers will need to enter into a similar contractual commitment with their network providers as for Type 1 Presentation Numbers – that they are entitled to use the numbers they have selected.

A2. Glossary

Anonymous Call Reject (ACR)	Where the called party has opted to reject calls where the caller has chosen to prevent the display of their CLI data.
Calling Line Identification (CLI)	Calling Line Identification is the data that is provided with a telephone call about the caller. It consists of the caller's line identity along with a privacy marking, which indicates whether the number can be shared with the recipient of the call.
Calling Line Identification (CLI) facilities	These are the facilities by which the telephone number of a calling party is presented to the called party prior to the call being established.
Connected Line Identity (COL)	Connected Line Identity is the data that is provided with a telephone call about the called party. It consists of the called party's line identity along with a privacy marking, which indicates whether the number can be shared with the caller.
Network Number	The Network Number is a telephone number that unambiguously identifies the line identity of the fixed access ingress to or egress from a Public Telephone Network or a subscriber or terminal/telephone that has non-fixed access to a Public Telephone Network. For CLI, it can also be the first known Public Electronic Communication Network in the call path, where the first known UK PECN does not reasonably trust the CLI data that is being provided or the CLI data is not available.
Network Termination Point	This is the physical point at which a subscriber is provided with access to a Public Electronic Communications Network and cab be identified by means of a specific network address, which may be linked to the Telephone Number or name of a Subscriber.
NICC	NICC is the UK telecoms industry standards forum that develops interoperability standards for UK communications networks.
Presentation Number	The Presentation Number is a number nominated or provided by the caller that can identify that caller or be used to make a return or subsequent call. It may not necessarily identify the line identity of the geographic source of the call