EDRi

EDRi's position on

THE PROPOSAL OF AN E-PRIVACY REGULATION

European Digital Rights | 20 Rue Belliard, 1040 Bruxelles, Belgium | Tel. +32 2 274 25 70 | www.edri.org

Contents

Proposed rules are necessary for individual's trust 1

Extending the scope of application of the new rules is necessary 1

European citizens want privacy by default 2

Cookie walls prevent users from giving consent freely 3

New methods for giving or declining consent to tracking 4

Exception for offline tracking of users is unacceptable 6

Permitted processing of electronic communication data 9

Public transparency about law enforcement access necessary 11

Enforcement by DPAs is an improvement 11

Collective redress mechanisms should be restored 12

Conclusions 12

On 10 January, the European Commission (hereafter: "Commission") published its proposal[1] for a new Regulation that would replace the ePrivacy Directive .

EDRi agrees with the Commission that additional rules are necessary to ensure trust in and the security of all types of electronic and digital communications. The Commission's proposal provides a solid basis, although several improvements are necessary.

Below you will find a brief explanation of EDRi's analysis supporting its position.

Proposed rules are necessary for individual's trust

1. **EDRi underlines the necessity of the proposed Regulation. Firstly, it is of utmost importance that internet users can rely on the confidentiality of their communications and the integrity of their devices.** Their communications deserve protection in order to give effect to the fundamental rights to privacy, personal data protection and freedom of expression. The ever-growing connectedness of devices will increase the need for clear rules on protection of the confidentiality of communications, both for individuals and for businesses. Secondly, EDRi considers the proposed Regulation will be a boost for innovation and economic growth in Europe. Without trust in the protection of our digital communications, internet users will be reluctant to use online services. A government survey in the USA, where similar legislation is unlikely, found that 45% of households had refrained from certain online activities in the previous year, due to privacy and security fears.[2]

Extending the scope of application of the new rules is necessary

2. Extending the scope of application to so-called over the top services is a logical response to the changing landscape of how people communicate. From the user perspective, there is no functional difference between sending a message by using a traditional SMS-service or by using services such as WhatsApp, Telegram or Signal. **Users therefore expect that the rules governing the confidentiality of communications apply not only to traditional telecommunications services, but also to services that are functionally equivalent, such as Instant Messaging and Voice over IP services.**

   However, extending the scope of application of the new rules should not lead to national (telecommunications) laws allowing law enforcement and intelligence agencies to undermine the effectiveness of any security technology, such as end-to-end encryption.

1 https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications

2 "Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities", US National Telecommunications and Information Administration, May, 2016. https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities

3. **The need for extending the scope of application also applies to machine-to-machine communications.** It is likely that, in the coming years, the number of devices in and around people's homes that continuously communicate with other devices and computer systems through the internet will increase rapidly. User trust (and, therefore, takeup of such services) will depend on the confidentiality of communications and the integrity of these devices.

4. **The proposal also extends the scope to so-called ancillary services. However, it is not clear what services will be covered under this term.** For example, during the presentation of the proposal by the Commission, an official said that messages exchanged between users in the messaging system of a social network would be covered, but messages exchanged between users in the timeline of the same service would not be covered. The proposed ePrivacy Regulation (ePR) applies to interpersonal communication services which is defined in Article 2, point (5) and recital 18 of the proposal for a Directive establishing the European Electronic Communication Code (EECC), which is being negotiated at the same time as the ePR proposal. The critical point in the ICS definition [EECC recital 18] is that the communication is transmitted to a finite number of natural persons that are selected by the sender of the communication. This will undoubtedly create some borderline issues with e.g. closed Facebook groups where the number of participants is also limited. **We propose to extend this concept to include all such communication channels to avoid any arbitrary distinctions.**

European citizens want privacy by default

5. **It is disappointing that the Commission did not choose to enforce a high level of privacy protection by default.** The proposal contains a provision that demands that end users be given the "option" to determine through software settings whether they allow third parties to access or store information on their devices. In other words, contrary to Article 25 General Data Protection Regulation (GDPR), **the concept of this proposal regarding the protection of the end-user is "privacy by option" instead of "privacy by design and default"**.[3] What is lacking is the obligation for hardware and software providers to implement default settings that protect end users' devices against any unauthorised access to or storage of information on their devices. It is baffling and contradictory that unauthorised access to a computer system is a crime under EU legislation (Directive 2013/40/EC) while, under this proposal, unauthorised access to an individual's computer system could be permitted by default. The definition of end user needs to be clarified so it does not lead to a situation where the buyer of a device (an employer) is able to give consent[4] on behalf of the user of the device (its employee) for purposes which are not related to the employer's contract with the seller of the device or with the service provider.

   An earlier leaked version of the Commission's proposal actually contained a 'privacy by default' provision. The Commission deleted this provision without providing any justification

3 Article 10 (1).

4 Regarding consent, it is interesting to note that although GDPR based processing on legal grounds **and** consent, ePR is based exclusively on consent.

for this change. This deviation from the privacy by design principle is at odds with what the vast majority of EU citizens actually want. A recent research report undertaken for the Commission showed that almost 90% of EU citizens want such privacy-friendly default settings.[5] Similarly, privacy by design and security by design requirements would prevent market failure in the area of the Internet of Things and connected devices. According to a leader of the semiconductor industry, NXP, "until countries have a liability and regulatory framework to address their vulnerabilities, these (connected) things will remain insecure."[6]

6. The proposal also contains the obligation for relevant software providers to inform users about the availability of relevant privacy settings upon first use of the software.[7] Unfortunately, the Commission has not provided any guidance or clarification on this information requirement. Users should always be able to make free and well informed decisions, as mandated by the GDPR. Therefore, **any technical means used to provide consent must meet the requirements for consent as stipulated in the GDPR**. Providing general information about the privacy settings during the first use of software that will have an 'all or nothing' impact for any future use, will most likely not meet the requirements of consent as provided for in the GDPR.

7. Also, if the normal functionality of services and 'smart' devices depend on the user's privacy settings that are set during first use, users would, in practice, be forced to accept settings that may negate their rights in order to make normal use of these services and devices. It should be clarified that setting up these privacy settings upon first use does not automatically result in valid consent within the meaning of the GDPR. It should at least be explained how and when these settings could constitute valid consent.

8. Finally, **users should not only be informed about the privacy settings during installation or first use of the software, but also at other moments when users make significant changes to their devices or software**. Such notices should also be provided, for example, when users reset their devices to factory settings.

Cookie walls prevent users from giving consent freely

9. EDRi welcomes the fact that the Commission now includes flexibilities regarding certain types of cookies and similar tracking technologies. Requiring explicit consent of users for tracking by the first party to obtain aggregated insight into the functioning and use of a service degrades the value of a request for consent to users. However, the current proposal of the Commission still allows for so called cookie walls. EDRi would like to make the following comments:

    a. **It is important that users be able to use a service without being tracked by third parties, especially if the user depends on, and has no real alternative to, this service.** Cookie walls preventing access to a service if users do not agree to terms of service should therefore be prohibited, especially when it comes to public services, services that

5 Flash Eurobarometer 443 (December 2016).
6 NXP, The internet of scary things, December 2016. http://blog.nxp.com/iot/the-internet-of-scary-things
7 Article 10 (2).

are financed by public funds or medical services. This should also entail a prohibition on the practice of excluding users who have ad-blocking or other applications and add-ons installed to protect their information and terminal equipment. On the basis of the provisions of the General Data Protection Regulation it is possible to argue that such cookie walls are not allowed at all, because a 'freely given' informed consent is lacking.[8] To avoid confusion and to provide legal certainty, it is important this be made explicit in this regulation.

b. **Allowing the storage of information on the user's equipment and reading information from the user's equipment for statistical purposes[9] is acceptable only when a number of conditions are met.** The resulting information may not, constitute a detailed picture of individual users and the information obtained must not be used for any other purpose than to obtain insight into the functioning and use of a service in an aggregated and general manner. The information shall not therefore be merged with other information to build a profile of a user, or be used to target the end-user in any way other than personalisation of a service that the end-user has explicitly selected. The proposal should be updated to include these conditions.

c. **End users may be confronted with forced consent mechanisms before they can use smart devices** (e.g. smart TVs) properly. In the context of the Internet of Things, it should be ensured that the functionality of smart devices is not conditional on consent as set forth in Article 8(1) of the proposed Regulation that is not necessary for the functionality requested. This particularises the conditions of Article 7(4) of the GDPR to the context of Internet of Things where end users buy and use physical products and reasonably expect certain functionalities of these products.

New methods for giving or declining consent to tracking

10. The Commission promises European citizens fewer cookie banners.[10] It is hoped that this goal will be achieved by developing new ways of expressing consent through browser settings.

    a. **According to recital 22, browser choices made by end-users should be binding on all parties.** This could mean that DNT (Do Not Track), which is an HTTP header field transmitted with every HTTP request that signals acceptance or rejection of tracking, gets a legal meaning that websites would have to respect, but this interpretation is not entirely clear from the proposal. What is clear is that recitals 22-24 use the possibility to technically block cookies in the browser as a way of expressing consent. Providers of web browsing software will be required to ask the end-user to select an appropriate cookie setting in the browser (e.g. accept or reject third party cookies), and this choice will constitute consent for all websites accessed.

8 See article 7(4) and recital 43 of the GDPR.
9 As meant with "web audience measuring" in article 8(1)(d).
10 This covers first-party cookies for self-hosted analytics like piwik, and it may also cover some commercial web analytics services where information obtained from first-party cookies is processed by a third party subject to a clear data processing agreement.

b. **Expressing consent in the browser in this way would eliminate most cookie banners, and websites can use cookies for all users since the browser will be left with the task of technically rejecting the cookies if consent is not given. The disadvantage is that this type of consent cannot meaningfully be informed consent in the GDPR sense.** Only the website visited by the end-user can provide information about the purpose of the different cookies. The browser can only give general information on the catch-all level that third party cookies can be used for tracking and pose a severe privacy risk. Therefore, consent under Article 9.2 will be much less informed than consent under 9.1 which directly refers to the GDPR. This is the disadvantage of moving consent from the website (the cookie banner) to the browser.

c. The idea that consent to tracking can be declined by rejecting cookies only works if the tracking is done through third party cookies. Many third party trackers use device fingerprinting instead of cookies, perhaps because some end-users regularly delete their cookies for privacy reasons. Device fingerprinting is also access to information in the terminal equipment (browser), and device fingerprinting is mentioned in recital 20. **Contrary to cookies, there is no generic way to technically block device fingerprinting in the browser (and hence decline consent) since there are so many different ways of carrying out device fingerprinting.**

d. There are other limitations with expressing consent through browser settings, even for cookies. The same cookie can be first party and third party, depending on the context. If a user visits facebook.com, a first-party cookie with the user id will be set and used for the Facebook login. This will not require consent because the cookie is needed to provide the service requested (Facebook). If the same user later on visits a website that uses Facebook third party tracking (e.g., thorugh "like" buttons, for example), the same cookie will now be a third party cookie. Whether this cookie is transmitted to Facebook, thereby allowing tracking of the end-user, depends on how blocking of third party cookies is implemented in the browser. Some browsers will transmit a cookie that has already been set, even if blocking of third party cookies is selected in the browser.

e. **The Commission proposal is likely to reduce the number of cookie banners, at least if they only use cookie-based trackers. However, choices for end-users may become more confusing, and by moving the handling of consent for cookies to the browser** (which the Commission believes is a "gatekeeper" between the end-user and the website), the European citizen is essentially left with the responsibility of defending herself or himself against tracking by blocking cookies. If websites start checking whether third party cookies are enabled, similar to current checks for certain advertising and tracking blockers, and display an annoying banner asking the end-user to allow cookies in order to access the site, end-users will for all practical purposes be coerced

into accepting cross-website tracking. This will have severe negative implications for the fundamental rights of citizens. It will be worse than the current cookie walls since the consent to tracking expressed through browser settings will apply to all websites.

f. Device fingerprinting is also used to track users across devices through statistical correlations, but increasingly internet users are now tracked across different devices through the use of persistent identifiers linked to their log in details for specific websites or apps, online services or social media identities. These marketing identifiers can also be linked to offline activities through the use of other data systems, such as supermarket loyalty cards, coupons or theme park wristbands. In addition, established telcos are purchasing ad targeting platforms and openly entering the data markets with a specific value proposition on bypassing devices and installed software, including browsers. It is unclear how the current proposals in the ePR focused on consent through the browser will deal with these developments.

Exception for offline tracking of users is unacceptable

11. **EDRi is deeply concerned about the proposed exception for tracking users of communication devices in public spaces in the physical world ("device tracking")**. This type of technology is already widely in use and is not limited to busy shopping malls but is also used, for example, to map traffic flows on roads. The collected data not only reveals the behaviour of passers-by, but also includes individuals living in the neighbourhood. Moreover, in some contexts, such as in the vicinity of a religious establishment, a medical clinic or a sex shop, this information should be considered to be sensitive by default. The European Commission allows for this type of tracking, provided there is some sort of notification to the user.[11] Such notification is problematic for several reasons:

    a. **Firstly, the notification to the user does not contribute to the essential protection of the rights and freedoms of the user. Logically, such an approach could only function on the basis of implicit consent, which is unacceptable.** An unsuspecting user may not notice the sign, or several signs for several surveillance projects, in the abundance of such signs in a busy area. In addition, in cases of large-scale application of such technology the user might be notified only at the outer edges of such an area, which would render the existence of the technology even more invisible.

    b. **Secondly, it is not possible for users to evade this type of tracking other than by switching off one of the basic functionalities of their own devices.**[12] **It is not reasonable to expect that a user turn off wireless internet access on his mobile phone, especially if the user wants to use internet connectivity that they are paying for through the purchase price of their phone and their mobile subscription.** That also includes functionality based on Bluetooth, such as a wireless headset for his mobile

11 Article 8(2)(b).

12 See also recital 18 which discusses consent: "Basic broadband internet access [...] [is] to be considered as essential services for individuals to be able to communicate and participate to the benefits of the digital economy. Consent for processing data [...] will not be valid if the subject has no genuine and free choice, or is unable to refuse or withdraw consent without detriment."

phone or the use of so-called *beacons*[13] in a store. An opt-out regime is not suffic, as it is cumbersome to the user. This breaches the principle of "freely given consent" established in the GDPR. Additionally, the user cannot be expected to opt-out - possibly multiple times - when entering an area where device tracking technologies are used.

c. Unlike the companies that offer such device tracking would like to make us believe, it is extremely difficult, if not impossible, to set up such a service in a way that the protection of privacy of bystanders is respected. Even if the collected data is "irreversibly encrypted" it is relatively easy to figure out whether a given user has been detected at a certain time on a certain location.

d. It is difficult to see why this form of use of location data deserves weaker protection. Elsewhere in the proposal, the Commission does not allow providers of communications services to process information about the location of the users unless those users have given their explicit permission.[14] It is not that this data in context of device tracking in a physical world could somehow be considered to be less sensitive.

e. **Finally, if it is technically possible to opt out, for example by registering the device WiFi MAC address in a database which the provider of the location-tracking service must check, the same method can be used for an opt in scheme.** Especially in high risk situations, where the end-user can be recognised (cross-linked with previous data captures) over time intervals of more than 24 hours, opt in should always be preferred over opt out. In either case, the leaked identifiers from the end-user device should never be stored and processed directly but only used as the basis for calculating new pseudonymous identifiers that cannot be cross-linked across different tracking services and which have a short persistence, limited to what is strictly necessary for providing the service. The requirement in Article 8.2.b to apply the technical and organisational measures in Article 32 of the GDPR should be supplemented with a mandatory data protection impact assessment.

12. **EDRi believes that the text around location privacy should be strengthened.** The current e-Privacy Directive was drafted with concerns about the expansion of location based services, at the time based on proximity to GSM phone masts. The Directive treats location data as a separate category with more stringent rules, requiring clearer information on processing and extra opportunities for opting out. The Directive has some problems in practice, as it is sometimes unclear whether some data should be treated as location or traffic, while data collected from GPS in mobile phones by apps and operating systems was not covered. **The proposed Regulation removes the special status of location, treating phone mast derived location as "communication metadata", which would not cover location from other sources** (Recital 17), such as GPS. **The text does not make clear how these other types of location data should be treated**, presumably as *information stored in and related to end-users' terminal equipment*, or content if transmitted.

13 See also recital 18 which discusses consent: "Basic broadband internet access [...] [is] to be considered as essential services for individuals to be able to communicate and participate to the benefits of the digital economy. Consent for processing data [...] will not be valid if the subject has no genuine and free choice, or is unable to refuse or withdraw consent without detriment."

14 Recital 17

The proposals would create a two-tier regulation for location data that would create confusion and privacy risks for end users. Data from devices could be processed without consent if it is "necessary for providing a service" (Art. 8(c)) but this can be hard to establish. **Location data from all sources should be given a high level of protection as it carries a high privacy risk, a fact acknowledged by regulators in many Member States**. The proposals seem designed to enable the current location data markets, with telecommunication and OTT services operating separately, but fail to acknowledge the convergence and aggregation of data sources. **Users should not be made responsible for understanding how their location was obtained and the various applicable regimes.**

Research by EDRi members[15] shows that most services built on location metadata are based on anonymisation, not consent, and have raised concerns that the data is not fully anonymised. Recital 17 acknowledges that tracking location may not be possible with anonymised data and may require the use of permanent identifiers. **The conclusion is that this is pseudonymous data and consent is required, but the Regulation should make this more explicit**, as it could have a major impact on current practices by mobile providers.

Therefore we recommend that:

a. Article 4 should be amended to include clear definitions of location data currently partially covered in Recital 17 (and possibly other sensor data as these can be used to calculate movement).

b. Article 8 should be amended to clarify the grounds for processing device location data - and possibly other sensor data - separately from the provisions designed for cookies and device fingerprinting. These grounds should exclude web audience measurement and be based clearly on consent for services, for example by using identical provisions as for metadata:

"the end-user concerned has given his or her consent to the processing of his or her device location data for one or more specified purposes, including for the provision of specific services to such end-users, provided that the purpose or purposes concerned could not be fulfilled by processing information that is made anonymous."

13. **EDRi recognises that location services can provide benefits to society, for example traffic planning in cities based on measurements of traffic congestion and travel times between different points in the city during the day. However, obtaining this information through tracking of individual citizens poses severe privacy risks and possibilities for abuse** (including the risk of mass surveillance by commercial or law enforcement entities). Citizens will not be able to verify whether the persistent identifiers emitted from their devices are processed in a way that limits tracking to what is strictly necessary for a purpose of genuine benefit to society, such as traffic planning in cities.

a. Moreover, given the pervasiveness of tracking in public spaces based on emitted device identifiers throughout the world (including countries where no data protections laws exist), device manufacturers are taking steps to mitigate this privacy risk through

15 https://www.openrightsgroup.org/ourwork/reports/mobile-data

technical means, for example randomisation of WiFi MAC addresses that are emitted from smartphones. Randomisation of emitted identifiers will gradually make tracking less and less effective. This is good for the privacy of individual citizens, but is also impacts negatively on location services of genuine benefit to society.

b. In most cases, there are better solutions to obtaining location-based information than centralised tracking of individual citizens. Smartphone apps can obtain the device location (e.g. through GPS) without leaking it to a third party. Smartphone apps can also easily calculate the travel time between points A and B in a city, and anonymise the information before it is submitted to a server. When the necessary linkage of two location measurements to calculate a journey time is done locally in the end-user device and anonymised, there is no privacy risk. In this way, the (smart) city will get the information necessary for traffic planning without tracking the individual citizens.

c. Technical solutions based on local computation in the end-user's device should always be preferred over centralised tracking. Therefore, the broad powers in Article 8.2 provides the wrong incentives to service providers that depend on location input and force citizens to defend themselves by turning off WiFi, or similar defensive measures, to both their detriment and that of the economy. Instead, the ePR should provide an incentive to develop technical solutions where citizens can provide location data to services without any privacy risks (privacy by design).

Permitted processing of electronic communication data

14. Compared to the current ePrivacy Directive, **the proposal increases the scope for processing metadata and content by providers of electronic communications services. EDRi has serious concerns that these changes can lead to voluntary data retention for all subscribers** on a level that may even be comparable to the mandatory data retention that the CJEU has ruled on in April 2014 (the Data Retention Directive) and December 2016 (national data retention laws).

    a. **With end-user consent, communications metadata can be processed for one or more specified purposes**, including the provision of services to the end-user. Unlike the current rules, the purpose does not have to be value added services of direct benefit to the end-user, but could, for example, be location tracking services for heatmaps and similar statistics (Recital 17). The way in which this consent is obtained and expressed should be carefully analysed to avoid invalid forms of consent not permitted by the GDPR, e.g., under over-broad terms and conditions, or through pre-ticked boxes in online contract forms.

    b. Article 6.1.b and recital 16 increase the scope for processing and storing metadata for security and quality of service (QoS) purposes by the provider of the electronic communications service. Article 6.2.a also allows processing and storage of metadata (via the exception in Article 7.2) for mandatory QoS requirements pursuant to the European Electronic Communication Code (EECC) and the Net Neutrality Regulation 2015/2120. It is important that metadata processed for security and QoS purposes is

anonymised as soon as possible, and that the storage of metadata is limited to what is strictly necessary for the purpose. The current proposal does not have sufficient data protection safeguards in this regard. For example, there is no clear requirement in the proposal that anonymised metadata should, to the greatest extent possible, be used for the purposes of network security and QoS.

c. **When can the content of communications be used by (some) third parties? (Article 6.3)** The content of communications can only be used ("processed") if the user "consents" to it. Again, we feel that the quality of this "consent" needs to be carefully checked, specifically as to whether, in the challenging context of the digital environment, the user is offered a genuine, free and fully informed choiceFurthermore, consent should be required for all communicating parties in the communication, except for narrowly defined IT-security purposes of protecting the recipient against computer viruses and clearly unsolicited messages (spam). Regarding safeguards, (recitals 18-19 have important restrictions which need to be put in the article. In any case, the use of consent in for the processing of the content of communications should be for exhaustively listed purposes that the legislature considers legitimate, that do not interfere with the right to private communications and that clearly benefit individuals and without being in the detriment of their communications with their contacts.

d. **Data protection impact assessment should be mandatory before communications metadata is stored for security and QoS purposes.** This should also apply to metadata processed and stored for fraud detection, as permitted by Article 6.2.b as well as the current ePrivacy Directive. Exceptions for major public interests must be better defined

15. Article 11 of the proposal allows Member States to restrict Articles 5 to 8 the proposal to the extent that these restrictions and exceptions are "necessary, appropriate and proportionate" to safeguard major public interests such as national security or the fight against crime. The legal meaning of this provision appears minimal, as it does not create new powers for Members States and merely reaffirms their authorities and obligations as mandated under the EU primary law.

16. This provision is similar to, and cross-refers to, article 23 in the GDPR. Similar exception clauses are also contained in the Data Protection Directive and the e-Privacy Directive. The clauses in the GDPR and this proposal are an improvement, in that they expressly add that such exceptions must "respect the essence" of the fundamental rights affected; a clear reflection of the wording of the European Charter of Fundamental Rights and recent CJEU case-law. The scope of these exception clauses have remained somewhat obscure, in particular in relation to national security. Under the abovementioned directives, these matters were naturally regulated in Member States' laws because the directives themselves had to be transposed into domestic law – but that fits less easily within a regime based on regulations that are, in principle, directly applicable in all the Member States, in a harmonised way. Consequently, **these exception clauses in the regulations again leave these matters first and foremost to be determined by Member States' laws – meaning that in these areas, the national laws will be different, allowing for more or less intrusive actions by national security-, defence and law enforcement agencies in the different Member States.** But, whereas under the 1995 Directive, there were rules regarding which national law was the "applicable law" in a transnational context (Article 4 of the Data

Protection Directive 95/46), there are no such rules in the GDPR nor in the ePD proposal. **This is particularly problematic in relation to activities by such agencies in the inherently borderless internet and wider digital environment**, including in relation to questions of when and subject to what conditions, safeguards and procedures such agencies can seek access to communications or device data in servers or devices in other countries or in the "cloud". This must be addressed in clearer rules than the vague derogation clauses now in the GDPR or, especially, this proposal.

Furthermore and in respect to the CJEU ruling[16] from December 2016, there should be explicit limits on the implementation of national data retention provisions. **The CJEU made it very clear that any legislation that does not limit the range of targets based on reasonable suspicion is unlawful, because it amounts to a violation of the principles of strict necessity and proportionality. We strongly recommend to add a provision in the proposal to address the unlawfulness of untargeted surveillance of EU citizens.**

Public transparency about law enforcement access necessary

17. Article 11.2 of the proposal stipulates that providers of electronic communications services should be able to provide the competent supervisory authority with information about the number of requests received from law enforcement agencies, the legal justification invoked and the provider's response. EDRi suggests to include an obligation for providers to make this information public in a meaningful aggregated format, including in the absence of a demand from the authority. **Transparency from providers on the extent and manner in which they share personal data of users with public authorities contributes to user confidence and supports academia as well as civil society organisations in evaluating national surveillance legislation.** We therefore recommend the inclusion of a provision for mandatory transparency reporting. Many providers already publish so called transparency reports. Some of those reports are limited to the requests received, while others explain the legal framework in which they operate.[17] The Commission's proposal offers the opportunity to include transparency about requests of law enforcement uniformly. EDRi would be in favour of such a transparency provision.

Enforcement by DPAs is an improvement

18. Data Protection Authorities will be in charge of monitoring the application of the proposed regulation.[18] Particularly due to the cooperation provisions in the GDPR, this is an improvement to the current situation, which allows for supervision to be placed in the hands of other authorities, such as telecommunication regulators. This will require changes in regulatory competences in some Member States, which we welcome.

16 CJEU Joined Cases C-203/15 and C-698/15 Tele2, Watson et al.
17 https://www.vodafone.com/content/dam/sustainability/2014/pdf/vodafone_full_report_2014.pdf
18 Article 18(1)

Collective redress mechanisms should be restored

19. **Article 21 in the proposal omits the right to collective redress, which was expressly included in an earlier, leaked version. We believe this to be both a serious omission** and one that undermines the principle that the provisions in the proposal "particularise and complement" those in the GDPR, which provides for several avenues for remedies. Here, they appear to actually leave out a major, important new mechanism for upholding data subjects' rights. Although Article 21.2 refers to this possibility for individuals or legal persons "having a legitimate interest", both the concept of legitimate interest and the inexplicable absence of a link to Article 80 of GDPR require further clarification. **We urge the reintroduction of the provision for collective redress and effective remedies proposed in article 23 of the leaked version from December.**

Conclusions

20. **The ePrivacy Directive is a necessary element in European regulation that required an urgent update, especially after the GDPR was passed.** During 2016, the European Commission launched a series of consultations, impact assessments and surveys which were carefully prepared, allowing for all stakeholders, including a significant number of citizens and civil society groups, to express their views. This analysis makes it clear how important privacy is individuals in Europe, also and especially in the digital environment, and what needs to be done to update the current rules. **The Commission has rightly identified out some of the key issues, but it is regrettable that the published text is considerably weaker than the earlier version that was leaked in December 2016.** Furthermore, given the fact that the definitions are cross-referenced to the European Electronic Communications Code, the co-legislator needs to be sure to keep both texts consistent and as privacy friendly as possible.

21. **Although the intentions of the Commission are laudable, the current text will need thorough work to ensure that the privacy, data protection and other fundamental rights of citizens are fully respected in the digital environment**, especially also by providers of e-communication networks and -services and OTT providers. A significant number of articles and recitals will have to be substantially modified if citizens' rights are to be appropriately protected and citizens' trust in the digital environment – and thus in the Digital Single Market – is to be assured. We hope the co-legislators will not fail the citizens, with unforeseeable negative consequences for individuals and businesses alike. Given the rapid development of certain technologies (Big Data, the Internet of Things), the **European institutions need to make an extra effort to ensure that privacy and confidentiality of communications of European citizens are not considered as a tradeable asset, but as a right to be strongly protected. This will generate the trust needed to ensure that Europe is a world leader in privacy-respecting technologies**.

EUROPEAN DIGITAL RIGHTS

European Digital Rights | 20 Rue Belliard, 1040 Bruxelles, Belgium | Tel. +32 2 274 25 70 | www.edri.org