6 March 2017

Recommendations of *La Quadrature du Net* on the revision of the ePrivacy directive

Executive summary

The 2002 ePrivacy Directive (ePR) aimed at specifying and complementing the former general data protection legislation (directive 95/46/CE) in the sector of electronic communications, in particular in ensuring "full respect for the rights set out in Article 7 and 8 of that Charter[1]. When the EU began to modernise the data protection framework in 2012, it first focused on the replacement of the old 1995 Directive by the General Data Protection Regulation (GDPR). The latter was finally adopted by the European Parliament on 26 April 2016. But from the beginning of the negotiations, the Commission made clear that this agreement should be followed by a revision of the 2002 ePrivacy Directive. The current revision of the ePrivacy Directive is not a simple harmonisation with the GDPR, but rather **a unique opportunity for a deep and ambitious update that goes beyond its current spectrum to cover current and future digital issues**.

While the debate about mass surveillance has been going on for the last three years, the Court of Justice of the European Union recently made important rulings on data retention. At the same time, scandals of tracking by service providers regularly make headlines, it is obvious that **the revision of the ePrivacy Directive is at the heart of the actuality.**

The **European Parliament's work on the ePrivacy legislation will be crucial in respecting the will of civil society** - a will that was first expressed by stakeholders through the Commission's consultation in Spring, and more recently by European citizens through a Eurobarometer so as to tilt the balance in favour of fundamental rights.

1 Recital 2, Directive 2002/58/CE

Below are the main issues that will be tackled in the negotiations:

1. GDPR and ePrivacy are both necessary

The European Commission didn't cave in to industry's pressure and to their call to repeal the ePrivacy Directive: a draft regulation was indeed presented on 10 January 2017 to replace the directive. However, it remains essential to keep repeating why this future legislation is useful and perfectly compatible with the GDPR.

- **Electronic communications need a special regime:** past years have seen the e-communications sector develop rapidly with the emergence of new technologies such as Internet-based messaging services. Digital communications are everywhere in our everyday life. The tools and services we are using to communicate are numerous and diverse: we often use several communication services on one device (SMS, email, online messaging, chat, etc.) or several devices. According to the 2016 Eurobarometer on ePrivacy: "Mobiles are by far the most frequently used communication device or service, with 74% of respondents using them daily". This is why we cannot protect the privacy of citizens without guaranteeing the confidentiality of their communications.

  For this reason La Quadrature du Net welcomes and supports the idea of Recital 2 of ePR : "The content of electronic communications may reveal highly sensitive information about the natural persons involved in the communication, from personal experiences and emotions to medical conditions, sexual preferences and political views.… Similarly, metadata derived from electronic communications may also reveal very sensitive and personal information. These metadata includes the numbers called, the websites visited, geographical location, the time, date and duration when an individual made a call etc."

- Moreover, **the ePrivacy Regulation will cover Article 7 of the Charter of fundamental rights of the EU:** "Everyone has the right to respect for his or her private and family life, home and communications", which is not the case of the GDPR.

- **Cookies, and more generally the confidentiality of a user's terminal equipment, are not directly covered by the GDPR:** contrary to what the advertising industry repeats, the ePrivacy Regulation is needed to address the issue of cookies and more generally of the security of devices. The General Data Protection Regulation only covers cookies indirectly because the definition of "personal data" has been enlarged and cookies as unique identifiers can therefore be considered personal data. However the security and the confidentiality of our devices should not be only indirectly addressed, and must be subject to strong protection through unambiguous provisions. The ePrivacy Regulation aims at this, and is therefore also needed here.

2. Equity principle between all actors

Extending the scope of application of the future Regulation to new e-communications services (the so-called OTTs - Over-The-Top services - or rather called "number-independent interpersonal communication services" - NICS) is necessary if we want on one hand a **high and homogeneous level of protection for all users** and on the other hand a level playing field for all service providers. European users do not know that the different services they are using are subject to different levels of regulation. If we want to ensure trust in digital services as well as a fair competition, there must be an **upward harmonisation of privacy standards.**

In a context of mass surveillance scandals and growing awareness of private tracking, European users are looking for protection and confidentiality. Therefore it would be unacceptable to reach equity among all services through a race to the bottom with respect to privacy in the electronic communication sector.

Nevertheless, La Quadrature du Net will pay much attention to the scope of the **derogation allowed to Member States for national security reasons which could block this upward harmonization** if it becomes too extensive. Indeed an equal level of obligation for all providers' electronic communication services should not permit national authorities to prevent or weaken some technologies ensuring security and confidentiality, such as end-to-end encryption (see point 7 of this document).

Finally, the draft regulation broadens the scope to services which enable communication as a minor "ancillary" feature (Article 4.2). However it is very unclear what "ancilliary services" covers. During the presentation of the draft regulation by the Commission on 17/01/2017, it was explained that messages exchanged over a timeline on a social network would not be covered. This is a faulty interpretation of what interpersonal communication services are, which needs to be fixed in the report that MEPs will discuss. La Quadrature du Net presses in its work on the European Electronic Code of Communication (EECC) for a distinction between "private" and "public" communications. The question that must be asked is: is the electronic communication of a public nature?

3. Processing of metadata by the service provider

As recital 17 stipulates, "this Regulation broadens the possibilities for providers of electronic communications services to process electronic communications metadata, based on end-users' consent". This orientation taken by the European Commission is **incompatible with the aim of the ePR, which is the protection of private life and of personal data in electronic communications**, and goes against the principle that metadata are as sensitive as - if not more sensitive than - the content of communications.

This concession made to industry seriously weakens the entire proposal, because it brings us back to an outdated system where companies try by all means possible to get the consent of the users through unfair

means (unreadable contracts, hidden information, requiring consent to have one's data exploited, etc.).

In order to mitigate this risk, La Quadrature du Net recommends:

- **to consider the starting point of any contractual relation as a non-consent**. Indeed most of the drifts regarding consent happen during the conclusion of a contract where the service provider is in an obvious position of power, and makes the user consent to anything and everything. It is therefore essential to add to point (c) of Article 6(2) (which enables processing of metadata based on consent) that the consent to process metadata cannot be collected during the conclusion of the contract. The initial contract must assume that the user refuses any metadata exploitation (other than what is necessary for billing, calculating interconnection payment, meeting mandatory quality of service requirements, etc.) and subsequently the service provider will be able to ask for consent to process communication metadata.

- to add an overall principle to the ePR stating that **wherever feasible, services should be provided by processing information that is made anonymous.** In other terms, if a service can be provided by using anonymous data, that must be done. Such a general principle would be a minimum to guarantee the main objectives of the Regulation, perfectly summarized in the title itself : "the respect for private life and the protection of personal data in electronic communications"

4. Protection of information related to end-users' terminal equipment

As we explained above, the so-called "cookie provision" finds its rightful place in the future ePrivacy Regulation (see point 1). However we should stop calling it "cookie provision" as this provision on "the protection of information stored in and related to end-users' terminal-equipment" covers much more than the simple cookies. If a nickname is needed we would propose **"device tracking provision".**

The current regime bases the use of processing and storage capabilities of terminal equipment on prior consent. We will always defend a system based on prior consent (opt-in) rather than on a right to opt out. However, it must be recognized that the current opt-in regime has been very badly implemented and needs reforms. Indeed, giving actual, informed and explicit consent rather than simply clicking an "Agree" button takes not only time, but the willingness and skills needed to understand the consequences of accepting. Going through this process every time one connects to a webpage is not possible.

We need to develop a new system that goes beyond mere consent. The Commission has developed in its proposal a new system that make it possible to **express consent by using appropriate settings of a browser or other application. This is an interesting orientation, but such a solution would be efficient and acceptable only under four conditions :**

- the proposal's wording needs to be clarified

The wording of the Commission's proposal about access to the terminal and collecting information from the terminal (art. 8.1 and related recitals 21 and 22) is not clear enough. This provision does not specify how users will concretely be able to consent to or refuse the use of processing and storage capabilities of terminal equipment via their browsers. It is essential to give as little leeway as possible to service providers, in order to see the ePR Regulation implemented in accordance with its fundamental objective: ensuring "the respect for private life and the protection of personal data in electronic communications".

- web audience measuring cannot be considered an exception

The Commission's proposal stipulates that access to information stored and in relation to a device shall be prohibited unless it is necessary to measuring a web audience.
Such an exception is understandable, but this provision must be complemented by strong safeguards. Today very few web audience measuring service providers exist, and all information society services are using the same tools, all owned by the same big firms. This is problematic when data collected by these big groups for different services are aggregated and sold for commercial purposes.

The web audience measuring exception should be better framed, and complemented with a safeguard stipulating that this can be only done for mesuring web audiences, and that web audience measuring service providers may not aggregate data collected on behalf of several clients.

- the obligation to consent should be abolished

Users should have the right to refuse being tracked. Forcing users to choose between paying for a service or obtaining the same service by providing personal information goes against the General Data Protection Regulation. This comes down to equating consent with monetary payment, and thus considers consent as compensation for a service. Affected individuals cannot truly consent to their data being used for advertising purposes if access to a service requires consent even when the service in question could be provided without advertising. If declining entails that the service must charge money, consent cannot be considered free, and thus is not valid.

To remain consistent with the GDPR, the banishment of the so-called "cookie wall" should be explicitly enshrined in the related article or in the related recital. Keeping such a possibility for information society service providers would seriously go against a general trend among European citizens. The last Eurobarometer on ePrivacy conducted by the European Commission and published in December 2016 revealed that: "Respondents think it is unacceptable to have their online activities monitored in exchange for unrestricted access to a certain website (64%), or to pay in order not to be monitored when using a website (74%)".

- new forms of device tracking should be limited

The Commission's proposal aimed at regulating new forms of tracking, especially those based on the collection of information emitted by terminal equipment to enable it to connect to another devices or networks. The answer brought by the **proposal is absolutely unacceptable and fails to tackle the challenges of these very intrusive new forms of tracking**.

The draft regulation enables companies to track users of communication device in public spaces in order to count people in a certain area, to send commercial messages when users enter stores, to analyse how users move in a specific area and if they return, etc. This provision clearly **crosses a red line in term of invasive tracking**. Information emitted by terminals are unique identifiers which will can localise individuals and record their movements in different areas of the offline world.

This provision is **all the more scandalous as these personal and sensitive data are collected without the user's awareness**. The tracking companies would only be obliged to display a "clear and prominent notice", but what does a "clear and prominent notice located on the edge of the area of coverage"[2] mean when the area is a public square? How to be sure that users have seen it? And even if everyone could see the notice and be informed, it is **unacceptable to track people by default, especially in public spaces.** It is easy to foresee that the process to stop the collection of data will be a real obstacle course that nobody would take the time to suffer.

This provision is a big step backward that fits neither with the general trend of the EU data protection legislation, nor with the expectations of European users (as a reminder: 71% of respondents to the ePrivacy Eurobarometer say "it is unacceptable for companies to share information about them without their permission, even if it helps companies provide new services they may like."), nor with recent national court decisions that clearly consider this practice as illegal.[3]

Prior consent should remain the only available rule regarding tracking. However, that being said, the principle of free, informed and explicit consent sets the limits of the current system, and in the context of such invasive forms of tracking it obliges us to rethink the actual structures in considering such alternatives as privacy by design and by default.

2 See recital 25 of the Commission's draft proposal

3 Wednesday 8 February the French Council of State sided with the French Data Protection Authority (CNIL) to confirm that JCDecaux - the largest outdoor advertising corporation in the world - was not allowed to collect device identifiers when users passed by its advertising boards. See the court decision (only in French) : http://arianeinternet.conseil-etat.fr/arianeinternet/getdoc.asp?id=209297&fonds=DCE

5. Privacy by design and by default

The principle of privacy by design and by default was introduced by the GDPR in its Article 25. It must now be followed in practice, and the ePrivacy Regulation is a perfect opportunity for that.

The European Commission suggested in a previous leaked version of the Regulation that "the settings of all the components of the terminal equipment placed on the market shall be configured to, by default, prevent third parties from storing information, processing information already stored in the terminal equipment and prevent the use by third parties of the equipment's processing capabilities". **This wording is in no way revolutionary: it is a concrete application of Article 25 of the GDPR** which would put an end to current unacceptable practices where companies (qualified as third parties) unknown to the users collect data about them without their knowledge (non-free and uninformed consent is not consent).

The advertising industry - seeing its very lucrative but unethical business practices endangered - lobbied the Commissioner's cabinets so strongly that this concept of privacy by default disappeared from the Commission's final proposal. **The Members of the European Parliament, representatives of the European citizens, now have the duty to reintroduce to the text this provision of privacy by default applied to tracking by third parties, and to put an end to this unfair and outdated practice.**

It is useless to hope to be competitive by engaging in the race to ever more intrusive tracking models. We must meet the challenge ahead and see in an ambitious and privacy-respecting regulation the necessary incentive to the sought-after innovation. But this change of orientation and change of companies' economic model will not happen thanks to free market competition. Without strong and ambitious regulation, companies will never agree to change their practices. The revision of the ePrivacy directive - and with it a provision for privacy by default - is the perfect occasion to promote this turning point which the digital economy needs so badly.

6. Consent

The Commission's draft regulation broadens the possibilities to process electronic communication metadata, based on users' consent. As explained in the point 3 of this document, this extension could be incompatible with this regulation's objectives of privacy and data protection. However, whatever happens with the article covering the processing of electronic metadata, the concept of "consent" is lacking important safeguards to make it truly effective.

As with the GDPR, the ePrivacy Regulation will guarantee that end-users "shall be given the possibility to withdraw their consent at any time". However the ePR should also ensure that **after the consent is withdrawn not only should all data processing stop, but all data should also be erased.** This must be a condition of consent-based data processing.

7. Restrictions for Member States

Article 11 gives the Member States the possibility to derogate to the obligations set up in Articles 5 to 8. To remain consistent with the GDPR, this article will be based on Article 23 of the General Regulation. La Quadrature du Net wants to remind MEPs that **the scope of this "Restrictions" Article in the GDPR remains too broad**: it permits Member States to use these ill-defined concepts of “public security” and “national security” whenever they find it convenient. Some of them used to do it for measures enabling general data retention (even after the CJUE declared them noncompliant in April 2014) and **they will keep using it to legitimise other measures infringing fundamental rights** that will require years for the CJUE to adjudicate, to the detriment of people who will suffer them in the meantime.

If MEPs cannot restrict it because of what has been adopted in the General Regulation, they should at least:

- add a provision reminding Member States that any legislative measures they take on the basis of this article should be in accordance with the Charter of Fundamental Rights of the EU, in particular with Articles 7, 8, 10 and 52.

- remain vigilant and uncompromising toward the potential coming changes of the Council which might try to extend the derogation for "national security" reasons.

8. Collective redress mechanisms should be guaranteed

The article about "remedies" (Article 21 in the Commission's proposal) lacks a paragraph on collective redress mechanisms. This essential provision - that enables users to mitigate the disproportionate power relationship between them and the service providers in enabling them to be represented collectively by a consumer or non-for-profit organization - was missing from the last leaked version of the draft regulation. The MEPs must reintroduce it to protect the rights of citizens and to remain consistent with Article 80 of the GDPR - provision that the MEP did support in 2016.

9. Sanctions

In terms of sanctions Article 93 of the GDPR applies to infringements of the ePR. The European Commission proposed a classification of the ePrivacy provisions according to the scale of infringements provided by the General Regulation. La Quadrature du Net deeply regrets the Commission's decision to consider infringements of the protection of end-users' terminal equipment as a moderate violation and to make them be subject to only moderate sanctions. Tracking devices is extremely intrusive and can lead to serious privacy violations,especially knowing that tracking technologies are on the rise and are becoming

ever more precise and invasive. One of the reasons to review the 2002 ePrivacy Directive was to take into account and to regulate new forms of tracking. We all know, however, that **regulating without strong dissuasive sanctions is useless. Therefore we must consider infringements of the "protection of information stored in and related to end-users' terminal equipment" tobe a most serious violation**, subject to the highest sanctions provided by the General Data Protection Regulation.

Contacts

Léa Caillère Falgueyrac – Legal and Policy Analyst

lcf@laquadrature.net