E-Privacy revision: An analysis from civil society groups

In light of the adopted General Data Protection Regulation (GDPR) the organisations mentioned in the end of this document would like to draw attention to the following elements to be taken into consideration for the upcoming review of the e-Privacy Directive (2002/58/EC)

I. General Issues

SCOPE:

The scope of and definitions in the e-Privacy Directive are broadly limited to providers of e-communication services. We believe that its successor should cover all processing of personal data relating to relevant online activities, insofar as not already specifically covered by the GDPR to an adequate degree of precision to ensure predictability and the protection of fundamental rights to freedom of expression and privacy. It is particularly important to address issues that arise from the interaction between the right to privacy and freedom of communication, especially the necessity to safeguard the confidentiality of communications. With appropriate changes updating the existing legislation, the new instrument would again "complement and particularise" matters covered by the main instrument (now the GDPR).

NATURE OF THE NEW INSTRUMENT:

The revised instrument should be a Regulation, for the sake of consistency with the GDPR, for predictability and for effective protection of fundamental rights. The new instrument (the "Complementary Regulation") must fully incorporate and respect the standards or requirements set in the GDPR, and achieve the aim of ensuring that all the principles and rules of the GDPR are fully applied in the online context in the same manner across the common market.

CORE PRINCIPLES:

The successor to the e-Privacy Directive should protect:

- the fundamental **right to confidentiality of communications**, enshrined in Article 7 of the Charter. The revised instrument should expressly clarify that this principle applies fully to any type of data relating to online activities and communications, including traffic and location data as currently defined in the e-Privacy Directive, as well as any similar data created or used in the online environment, such as location data, browsing data, e-book usage patterns, mobile app use, search queries, etc. and any new data produced therefrom;

- the fundamental **right to protection of personal data**, as enshrined in Article 8 of the Charter;

- the fundamental **right to freedom of expression**, as enshrined in Article 11 of the Charter. To achieve this goal, the revised instrument should also protect the freedom to seek information, without being obliged to consent to tracking of one's information-collecting activities. This is particularly important when accessing information regarding issues linked to the special categories of personal data as set out in the GDPR.

- in addition, it is important to reaffirm **the fundamental right to the inviolability of a person's property**, with specific reference to the devices used for online activities, such as computers, mobile phones, laptops, etc. [*See below*].

- Any interference with these rights foreseen under the revised instrument must be in line with Article 52 of the Charter of Fundamental Rights. Such interferences, if introduced, must be clearly defined in law which is non-discriminatory and non-arbitrary and foreseeable in its application, and "necessary" and "proportionate" to genuinely achieve a clearly-defined objective of general interest. Such interferences should not in any way undermine the essence of the fundamental rights protected under the revised instrument. Individuals affected by them must have an effective remedy in accordance with Article 47 of the Charter.

These principles become all the more urgent in the online environment, since electronic communications have become such an integral part of many aspects or citizens' lives, whether economic, social, political or recreational. A successor to the e-Privacy Directive should acknowledge that online communications technology has such a profound impact on fundamental freedoms that it justifies specific applications of the principles of the Charter of Fundamental Rights, in order for the essence of these rights to be respected in practice. As the US Supreme Court put it eloquently in Riley v California (573 USSC (2014) 13-132, 25 June 2014, p. 17):

"Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person. The term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, Rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers."

The above quotation underlines that technology-independent legislation, while sounding attractive in theory, in practice is likely to fall short of any of the objectives above. When we argue in favour of technology-independence, it is about independence of the technological means through which fundamental rights are impacted, not about treating actors equally regardless of the impact they have on fundamental rights.

APPLICABLE LAW IN THE ONLINE ENVIRONMENT:

The question of applicable law in the online environment and the co-existence of EU and national legislation in this area is a crucial element that needs to be addressed. Although the original GDPR proposal aimed at harmonising the EU data protection measures falling within its scope (by virtue of it being a Regulation rather than a Directive), the final version of the legislation contains numerous provisions that defer to the Member States for their implementation and interpretation. Despite this, however and unlike Directive 95/46/EC, the GDPR does not contain an "applicable law" provision. This is especially problematic in the online context and should be remedied in the revision process of the e-Privacy Directive.

We propose to include in the revised instrument a provision on the lines of the one in the Directive 95/46/EC, i.e.:

> *1. Except as provided for in paragraphs 2 and 3, where the GDPR allows for matters to be regulated by the law of the Member States, each Member State shall apply the relevant national provisions to the processing of personal data carried out in the context of the activities of an establishment of the controller on the territory of the Member State.*

2. *When the same controller is established on the territory of several Member States, the processing shall be subject only to the relevant legal provisions of the Member State where the controller has its main establishment, as defined in article 4 of the General Data Protection Regulation, insofar as the decisions on the purposes and means of the processing are taken by the main establishment, and the main establishment has the power to have such decisions implemented, also by other establishments of the controller in other Member States. However, if the decisions on the purposes and means of the processing are taken by another establishment in another Member State, and the latter establishment has the power to have such decisions implemented, paragraph 1 shall apply.*

3. *When the controller is not established in the Union but the processing by that controller is subject to the GDPR and this Regulation*[1]*, the processing shall be subject to the legal rules relating to the matters covered by paragraph 1 of the Member State where the controller has appointed its representative.*

Specific issues

REVIEW VALUE-ADDED SERVICES:

References to "value added services" and "publicly available communication services" need to be reviewed in the light of recent technological developments. There is a need to clarify the difference between value added services **for the user** and data re-use for the benefit of third parties.

More broadly, appropriate changes are needed to address the fact that there is substantial substitution ongoing between internet-based services and more traditional "publicly available communication services". For example, SMS messaging over mobile networks has been largely substituted by instant messaging services. It therefore stands to reason that such service providers should have a similar responsibilities as more traditional communications service providers. This is not just for reasons of competition, but also needed in order to ensure ongoing protection for Charter rights.

ALIGN DEFINITIONS:

All relevant definitions should be aligned with the GDPR, and all concepts defined in the GDPR should be read in exactly the same way in the new Complementary Regulation.

TRAFFIC- AND LOCATION DATA AND OTHER GEOGRAPHICAL INFORMATION:

Geographical information, traffic data, location data and any other personal data processed should be reduced to the least-precise (least-granular, least-invasive) type needed for the relevant (initial or subsequent) purpose for which they are collected and used, and deleted as soon as they are no longer needed for the initial or subsequent purpose, in line with the principles of "data minimisation" and "purpose limitation," as defined under the GDPR. While these principles are already provided for under the GDPR, it is important to spell this out in the revised instrument for sake of clarity and precision, given the increasing use of geographical location data in many different contexts, and the serious intrusions of privacy that can result from the processing of location data. We draw attention in particular the following points:

[1] Because the controller offers goods and services to data subjects in the Union, or monitors their behaviour within the Union: vis Article 3.2 of the GDPR.

- Some data can be both location and traffic data, depending on the context. There is a need for more clarity on the particular regime that applies, ensuring maximum protection at any stage. Data derived from traffic, location or subscriber information should also be recognised as being covered by the Charter right to confidentiality of communications, in addition to the requirements of the GDPR.

- Regarding anonymisation, the opinion of Article 29 Working Party (Opinion 05/2014) on this regard should be taken into account.

- There are special difficulties in the de-identification of location data that were not apparent when the current directive was written. On the whole, data science is showing that yesterday's surefire methods for anonymisation are, in fact, simply pseudonymisation. The European Data Protection Supervisor, in his Opinion 7/2015 correctly argues that it "will be ever easier to infer a person's identity by combining allegedly 'anonymous' data with publicly available information such as on social media". Therefore, it would desirable not mentioning anonymisation if that is not what the measure offers.

- What data is retained for billing needs tightening. This is currently open to abuse, for example some operators keep detailed web history logs with the argument that they may be challenged on data charges. There is a need for more consistency and transparency over retention periods, and for full data minimisation in that context.

BEHAVIOURAL ADVERTISING, ONLINE TRACKING/COOKIES:

There is a need for new, clearer rules on the use of technical mechanisms for what is often called behavioral advertising. Behavioral advertising is in itself a misleading term, because current practices mostly rely on tracking across different websites, apps and even devices. This means that the focus lies on tying the identity of visitors across different contexts together in order to create vast, extensive profiles of individual citizens, with little transparency on what data are merged and what new personal data are generated on the basis of assumptions gleaned from that data. At the time of the drafting of the e-Privacy Directive, the mechanism of choice for this activity was the cookie. Currently, this is done through a wide array of mechanisms, at the same time as the online economy has, for the most part turned into a surveillance economy.

It is therefore clear that future legislation requires clear distinctions to be made between technical mechanisms that are used to recognise a user for the correct functioning of the online service (e.g. remembering that a user is logged in, that they have placed something in a shopping basket, etc), and those which are used for the purpose of mapping and analysing an individual's behaviour. The use of tracking, especially cross-context, should by its nature be regarded as constituting "monitoring of the behavior" of the data subjects concerned, and therefore be subject to the rules on such monitoring in the GDPR, in particular Articles 21 (right to object) and 22 (automated decision-making). In the context of new technical developments, in particular in mobile technologies and browsers, attention needs to be focused more on potential impact of these developments on fundamental rights and less on the specific mechanisms used. It should not be the case, for instance, that tracking performed with the assistance of application programming interfaces or javascripts are permissible without user consent, even though effectively identical tracking through the use of cookies without consent is prohibited. The new rules should simply prevent any tracking of the user's behaviour, which is not necessary for providing the service, without his/her consent (in line with the GDPR rules on profiling).

Generally, we support the implementation of the recommendations of the Article 29 Working Party in this regard. The new, clearer rules should have a focus on reducing the number of cookie consent re-

quests that the average citizen encounters during the day, and introducing more comprehensive and effective measures, as discussed below. This could be achieved *inter alia* by excluding innocuous analytics applications from the restrictions.

INSTALLATION OF SOFTWARE/MALWARE:

The revised instrument should explicitly clarify that the commission of any of the offences listed in Chapter II, Section 1, of the Council of Europe Cybercrime Convention (CETS No. 185) – i.e., unauthorised access to a computer system, interception of computer data, data interference or system interference, and misuse of devices – when perpetrated in relation to any computerised device, including mobile phones, tablets, laptops and personal computers, constitutes a violation of the fundamental right to the inviolability of a person's property as well as, in most cases, a violation of the person's right to data protection and confidentiality of communications. Authorisation for any such actions by any state agency should therefore be fully in accordance with the Cybercrime Convention and the Charter and based on clear, precise, published law that is foreseeable in its application, clearly serves a narrowly-defined legitimate public interest, and limited to what is necessary and proportionate to achieve that purpose. Member States should also prohibit and criminalise such actions by private actors in accordance with the Cybercrime Convention. They should not encourage such actions by private companies, e.g., to counter copyright infringements in what has been called "privatised law enforcement", but rather, should regulate such matters in clear public law meeting the above standards.

More specifically:

- The tracking of users across multiple websites and devices is highly problematic and intrusive. The tracking of users across multiple websites makes it impossible for users to foresee the parties who will gather knowledge about their internet use (and the extensive personality, health, sexual, financial, political and other data that can be extrapolated from such information) and the purposes for which that knowledge will be used. It follows from this that internet users are inherently incapable of giving informed consent to such tracking across multiple websites and devices.

- The denial of consent to a tracking cookie should not result in denial of any public service or a service for which the provider holds a dominant position. A public service should, by definition, be available to the general public and availability should not be based on the acceptance of a tracking cookie.

- Public and private-sector entities which offer healthcare, or advice in healthcare or other information regarding the issues linked to special categories of personal data as set out in the GDPR should not be allowed to use tracking cookies. Tracking cookies in relation to the delicate nature of the work of these entities may lead to the collection of highly sensitive personal data and -profiles, or such data or profiles can be inferred from the collected data.

SECURITY MEASURES

Privacy by default and design should be required by the new instrument to ensure privacy and confidentiality of communications. It should not be permitted to remove or weaken – or attempt to remove or weaken– any security measures that are applied by users, subscribers or third-party services. Transparency should also be required with regard to any inherent or discovered vulnerabilities with regard to such security measures.

CONSENT FOR THE PROVISION OF DATA FOR VALUE-ADDED SERVICES:

The e-Privacy Directive allows the processing of traffic and location data for value-added services with the consent of the data subject. There is the need to redefine what "value-added services" mean, from the user's perspective and that such consent, in any case, must fulfill the conditions set out in GDPR. Rules on how this consent needs to be provided (and revoked) should be made clearer. In some instances, this is resolved by the provider of the value-added service "conveying" the consent to the provider of the e-communication service, typically by issuing a warranty to the effect that the former

will only request the relevant data from the latter, in cases in which the former has such consent. Clearly, this means that the added-value service provider should bear the burden of proof if this is challenged.

Consent must not be bundled to cover both marketing communications and value-added services in one check box, as now sometimes happens. Smart, context-specific solutions can be found.

THE NEED FOR HARMONISATION OF THE "NATIONAL SECURITY/PUBLIC ORDER/CRIME PREVENTION ETC. EXEMPTIONS":

The exemptions in Article 15 of the e-Privacy Directive need to be harmonised – or they should be made subject to the "applicable law" rules proposed earlier. Jurisprudence from the Court of Justice of the EU in the *Digital Rights Ireland* Case should be reflected in clarifications of the safeguards that need to be in place when adopting measures that rely on the exemptions set forth in Article 15. The current wording has led to different restrictions (different exceptions to the main rules) in different Member States. This is especially problematic when those different rules are applied in the online context – both as concerns state measures relating to state security, public security, national security and against online crime and as concerns private-sector activities against such matters. Adoption of "applicable law" rules along the lines proposed above would resolve this, but it would be important to clarify that those "applicable law" rules also apply to sMember States' laws based on the "national security/public order/crime prevention etc. exemptions".

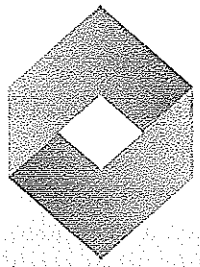
More specifically, it should be clarified in the successor instrument that, while the activities of the Member States in relation to national security are outside EU law, the disclosure of personal data by entities subject to EU law, and more in particular by EU data protection law, to the agencies of the Member States involved in national security matters *is* subject to EU law and EU data protection law – and in relation to online activities thus to the GDPR and the successor instrument, including the exemption clauses in the GDPR and the successor instrument. Such disclosure must therefore again be based on clear, precise, published law that is foreseeable in its application, clearly serves a narrowly-defined legitimate public interest, and limited to what is necessary and proportionate to achieve that purpose.

ENFORCEMENT:

- Data Protection Authorities, not Telecoms Regulators, should be in charge of enforcing the successor of the e-Privacy Directive. Irrespective of whether or not some telecoms regulators have done a good job in implementing the existing legislation, we are convinced that the new legal framework would make it more efficient for this role to be entrusted to Data Protection Authorities. This will ensure more consistency due, for example, to the DPAs' more detailed awareness of, and involvement in preparation of opinions and guidelines issued by the Article 29 Working Party or the European Data Protection Board. Furthermore, if the scope of the successor of the Directive is expanded to all online activities, as we propose, the enforcement would fall beyond the scope of the Telecoms Regulators. Lastly, the Telecoms Regulators are not and cannot be involved in the crucially important "cooperation"- "mutual assistance"- and "consistency" mechanisms introduced by the GDPR – which should fully apply to the new instrument replacing the e-Privacy Directive.

- DPAs should receive better tools to engage with technical standardisation processes, which should ensure more effective implementation of privacy by design.

This document was prepared by:



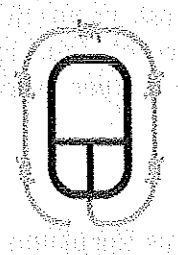
EDRi

PROTECTING DIGITAL FREEDOM

fipr

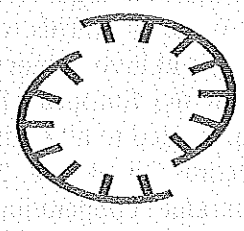
accessnow

PRIVACY INTERNATIONAL



BITS OF FREEDOM

VERDEDIGT DIGITALE BURGERRECHTEN



PANOPTYKON FOUNDATION