E-Privacy Regulation- Areas of Concern for the Open Rights Group

Javier Ruiz <javier@openrightsgroup.org>

These notes outline our main concerns with the current discussions in Brussels around the proposed E-Privacy Regulation, and have been presented ot the DCMS team responsible for the UK side of the negotiations. The contents have been prepared in partnership with our Danish civil society colleagues at IT-POL and are endorsed by the European Digital Rights Initiative.

ORG and other civil society organisations were quite pleased with the positions adopted in October 2017 by the European Parliament's LIBE Committee in its report on the ePrivacy Regulation. The amendments improved the original proposal by strengthening confidentiality requirements for electronic communication services, and include a ban on tracking walls, legally binding signals for giving or refusing consent to online tracking, and privacy by design requirements for web browsers and apps.

We are very concerned that the proposals so far presented for the Council of the European Union to adopt in its "general approach" are in direct conflict and seek to reverse most of these positive measures. Adopting this approach would lead to a reduction in the protections available to citizens and would cause potential conflicts with GDPR.

These notes are based on the draft text from the Austrian Council Presidency 13256/18 from 19 October 2018.

1. Further processing of electronic communications metadata

The current ePrivacy Directive only allows processing of electronic communications metadata for specific purposes given in the Directive, such as billing. The draft Council ePrivacy text in Article 6(2a) introduces further processing for compatible purposes similar to Article 6(4) of the General Data Protection Regulation (GDPR). This further processing must be based on pseudonymous data, profiling individual users is not allowed, and a data protection impact assessment must be carried out, which may require consultation of the Data Protection Authority in accordance with Article 36(1) of the GDPR.

Despite these safeguards, this new element represents a huge departure from the current ePrivacy Directive, since the electronic communications service provider will

determine what constitutes a compatible purpose. The proposal comes very close to introducing “legitimate interest” loophole as a legal basis for processing sensitive electronic communications metadata. Formally, the further processing must be subject to the original legal basis, but what this means in the ePrivacy context is not entirely clear, since the main legal basis is a specific provision in the Regulation.

In other words, once we exclude consent or a legal mandate, the original purpose of processing can only belong to a closed list of purposes listed in Article 6 such as processing for billing or calculating interconnection payments or maintaining or restoring the security of electronic communications networks. The addition of an open ended “compatible purpose” is in complete contradiction with the fundamental approach of Article 6 of the Regulation and would create legal uncertainty.

An example of further processing could be tracking mobile phone users for “smart city” applications such as traffic planning or monitoring travel patterns of tourists via their mobile phone. Even though the purpose of the processing must be obtaining aggregate information, and not targeting individual users, metadata will still be retained for the individual users in identifiable form in order to link existing data records with new data records (using a persistent pseudonymous identifier).

In our research on the use of data by mobile companies for analytics[1], of the kind envisaged here, we found that pseudonymous profiles were being created and these could be relinked to the user if she queried her bill. Giving companies the loophole proposed in the Council would lead to widespread abuse.

In addition, the situation becomes a form of voluntary data retention. The mandatory safeguard of pseudonymisation does not prevent the electronic communications service provider from subsequently identifying individual users. if law enforcement authorities obtain a court order for access to retained data on individual users.

2. Tracking walls and tracking without consent

The European Parliament introduced a ban on tracking walls, that is the practice of denying users access to a website unless they consent to processing of personal data via cookies (typically tracking for targeted advertising) that is not necessary for providing the service requested.

The Council text goes in the opposite direction by specifically allowing tracking walls in Recital 20 for websites where the content is provided without a monetary payment if the website visitor is presented with an alternative option without this processing (tracking). This could be a subscription to an online news publication. The net effect of this is that personal data will become a commodity that can be traded for access to online news media or other online services. On the issue of tracking walls and coerced consent, the Council ePrivacy text may actually provide a lower level of protection than Article 7(4) of the GDPR, which specifically seeks to prevent that

1 https://www.openrightsgroup.org/about/reports/mobile-data

personal data can become the counter-performance for a contract. This is contrary to the stated aim of the ePrivacy Regulation.

The current proposal in front of the Council also includes an addition to Recital 21 that would remove the need for consent altogether to store cookies, use of processing or collection of data when it may be:

"necessary for providing an information society service, requested by the end-user, that is wholly or mainly financed by advertising provided that, in addition, the end-user has been provided with clear, precise and user-friendly information about the purposes of cookies or similar devices and has accepted such use."

Facebook have argued that while users can have a fair degree of control over who sees their posts, they cannot choose what the company does with their data internally, on the basis that such processing is required for financing the whole enterprise through advertising. This is hotly disputed, but the current proposals seem designed to legitimise Facebook's position.

This incoherent addendum, which should be removed wholesale, would create huge confusion in an already unsatisfactory situation. The requirement that a user has "accepted" the use of cookies or similar devices is dangerously close to simply creating a backdoor for a much lower form of consent than in GDPR, or indeed in the rest of the Regulation.

The information requirements presented are also lower than those in Article 13 of GDPR, but even with these lower requirements, as explained in our request to the ICO for an investigation on online advertising, it is almost impossible for anyone to explain what happens to the data.[2]

Privacy settings and privacy by design

The Commission proposal requires web browsers to offer the option of preventing third parties from storing information in the browser (terminal equipment) or processing information already stored in the browser. An example of this could be an option to block third party cookies.

The Council text proposes to delete Article 10 on privacy settings and related recitals. The effect of this is that fewer users will become aware of privacy settings that protect them from leaking information about their online behaviour to third parties and that software may be placed on the market that does not even offer the user the possibility of blocking data leakage to third parties.

The arguments presented by the Presidency about the impact on users consent fatigue should be addressed by introducing mandatory privacy protections by default and technical solutions such as Do Not Track (DNT) to reduce the number of

[2] https://brave.com/ICO-Complaint-.pdf See also https://brave.com/adtech-data-breach-complaint/Behavioural-advertising-and-personal-data.pdf

consent requests in the online environment, not by removing user choice and information at the time of installation. This is an astounding sleight of hand that signals to industry that lower privacy settings should be the default.

3. Data retention

Article 15(1) of the current ePrivacy Directive allows Member States to require data retention in national law. Under the case law of the Court of Justice of the European Union (CJEU) in Digital Rights Ireland (joined cases C-293/12 and C-594/12) and Tele2 (joined cases C-203/15 and C-698/15), this data retention must be targeted rather than general and undifferentiated (blanket data retention). In the Commission proposal for the ePrivacy Regulation, Article 11 on restrictions is very similar to Article 15(1) of the current Directive.

In the Council text, Article 2(2)(aa) excludes activities concerning national security and defence from the scope of the ePrivacy Regulation. This includes processing performed by electronic communications service providers when assisting competent authorities in relation to national security or defence, for example retaining metadata (or even communications content) that would otherwise be erased or not generated in the first place. The effect of this is that data retention for national security purposes would be entirely outside the scope of the ePrivacy Regulation and, potentially, the case law of the CJEU on data retention. This circumvents a key part of the Tele2 ruling where the CJEU notes (para 73) that the protection under the ePrivacy Directive would be deprived of its purpose if certain restrictions on the rights to confidentiality of communication and data protection are excluded from the scope of the Directive.

If data retention (or any other processing) for national security purposes is outside the scope of the ePrivacy Regulation, it is unclear whether such data retention is instead subject to the GDPR, and must satisfy the conditions of GDPR Article 23 (which is very similar to Article 11 of the proposed ePrivacy Regulation), or whether it is completely outside the scope of EU law. The Council text would therefore create substantial legal uncertainty for data retention in Member States' national law, undoubtedly to the detriment of the fundamental rights of many European citizens.

4. Communications data only protected in transit

We are concerned about restricting the scope of the Regulation to data "in transmission", as proposed in the current Council text.

Restricting protections for communications at rest to GDPR would cause many problems and uncertainty. For a number of modern electronic communications services, storage of electronic communication data on a central server (instead of on the end-user device) is an integral part of the service. An example is the transition from SMS (messages are stored on the phone) to modern messenger services such as WhatsApp or Facebook Messenger (stored on a central server). This makes it

important that the protection under the ePrivacy Regulation applies to electronic communications data after it has been received, wherever it is stored.

The definition of “receipt of the content of the electronic communication” in recital 15a of the Council text could create some legal uncertainty for providers of electronic communications services because it is very unclear when end-users gain control over the individual messages, which is the trigger point for moving the legal protection of the content of the message from the ePrivacy Regulation to the GDPR. On most modern electronic communications services, messages are generally not “collected from a server” (as assumed by recital 15a), but rather stored on the provider’s servers after the transmission of the message, notified to the end-user on various devices (computers, smartphones, smartwatches, etc), and subsequently read and interacted with by the end-user on one or more of these devices.

5. Time to implementation

The Regulation should be applicable within a short timeframe if it is to be part of the UK legal regime after Brexit. Given the current delays a 24-month adaptation period is excessive.