astrea

Proposal for ePrivacy Regulation

-Balancing the interests of stakeholders in today's Digital Single Market-

By Steven de Schrijver, Partner, Astrea

astrea

Webinar Overview

1. Current Framework
2. Proposal for ePrivacy Regulation
3. Criticism and questions

astrea

Current Framework

- Directive 2002/58/EC on privacy and electronic communications

- Content
  - security of services
  - confidentiality of information
  - data retention
  - location /traffic data
  - unsolicited commercial messages
  - cookies

- Drawbacks
  - evolution electronic communication services **not** covered (e.g, instant messaging, voice over IP and web-based e-mail)
  - rules are too vague which led to differences in national implementations
  - unequal protection between Member States

astrea

ePrivacy Regulation Proposal

OBJECTIVES

1. **Update current rules** to take into account technological and market changes and extend the scope to all electronic communications providers
2. **Reinforce trust and security** in the Digital Single Market by enhancing the security and confidentiality of communications
3. **Create new possibilities** to process communication data
4. **Address inconsistent enforcement** and fragmentation at national level
5. **Align the rules** for electronic communications with the new standards of the **EU's General Data Protection Regulation (GDPR)**

astrea

ePrivacy Regulation Proposal

KEY POINTS

1. A **Regulation**, not a Directive
2. Widening of the territorial, personal and material **scope**
3. New **business opportunities** (when consent is obtained)
4. Simpler rules on **'cookies'**
5. Broader **protection against Spam**
6. EU-wide **harmonization** and **enforcement**
7. Increased **Fines**

Regulation, no Directive

The ePrivacy Regulation is not a Directive

Consequences:

- Direct applicability in the EU Member States
- No national legislation required
- Ruduction of risk of different implementation and application in different territories
- Same approach as for GDPR

Territorial Scope

Under the Directive:

"This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community." (Article 3)

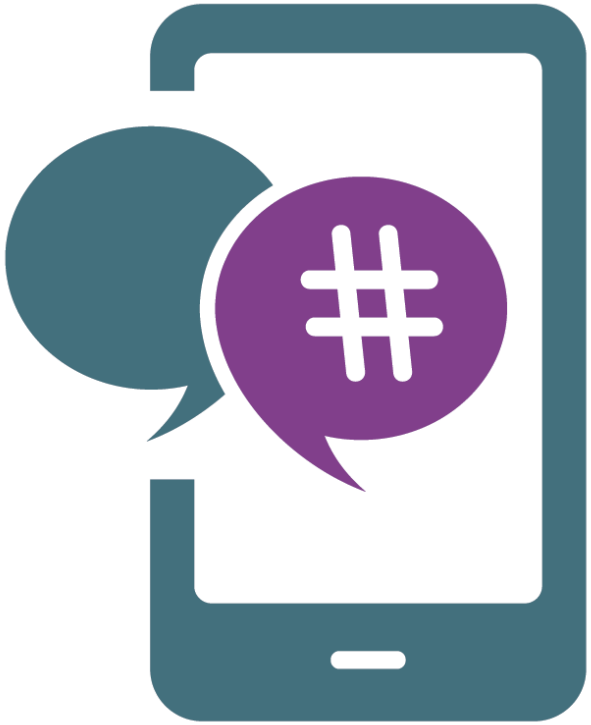
=> unclear, because never properly addressed by the CJEU

Under the proposed Regulation:

Data processed in connection with the provision of ECS in the EU **EVEN IF THE PROCESSING DOES NOT ACTUALLY TAKE PLACE IN THE EU**

Consequence: ECS from outside the EU may be required to exclude EU users and 'geo-block' the EU geographical area until they have complied with the new EU regulations.

Personal Scope



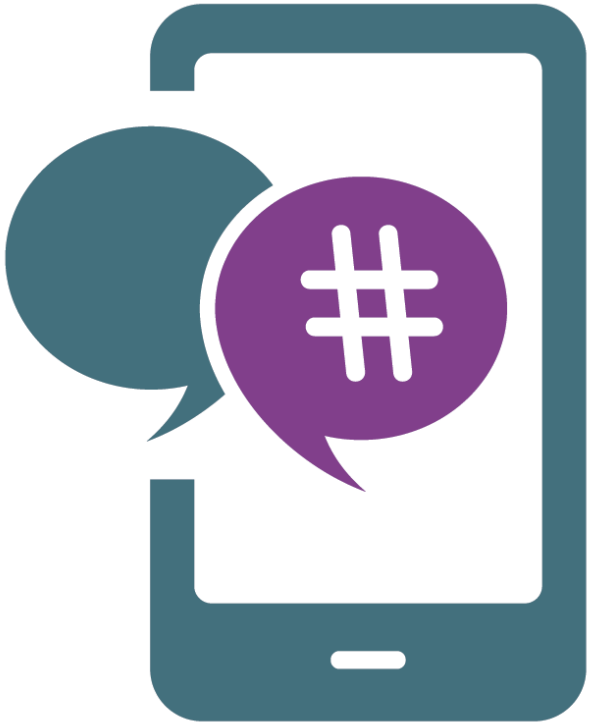
- New Principle:

  Confidentiality of consumers' communications**,** **irrespective of the technology used**

- new ECS providers, such as internet-based voice & messaging services, the so-called OTT or *over-the-top* services (e.g. WhatsApp, Facetime, Skype, iMessage, etc.)

- machine-to-machine communication (in light of IoT)

Personal Scope



- <u>Under the Directive</u>:
  - Providers of “publicly available electronic communications services” (i.e. traditional telecom operators)
- <u>Under the proposed Regulation:</u>
  - Traditional telecom operators
  - Providers of publicly available directories
  - Software providers permitting electronic communications
  - Natural and legal persons who use ECS to send marketing material

Material Scope

Under the Directive:

- **content** of electronic communications.
- **traffic/location data**:
  - not the primary aim
  - only limited protection under the Directive
  - often disregarded by Member States

Material Scope

Under the Proposal:

both **content <u>and</u> metadata** (e.g. timing, location and duration of the communication) derived from electronic communications

'metadata':

- wider than traffic/location data
- legal recognition
- still less stringent than content protection (*infra*)

Confidentiality

Article 8:

- Electronic communications shall be confidential
- Interference with electronic communications data is prohibited unless permitted by Member State or EU law.

Article 11:

- Restrictions are allowed to safeguard one or more general public interests specified in Articles 23 (1) (a) to € of the GDPR such as to safeguard national security.
- ECS providers must provide information to relevant supervisory authority on demand about internal procedures, number of requests received, legal justification invoked and their response.

astrea

Permitted Processing of Electronic Communications Data

Article 6.1:

Processing of electronic communications **data (general)** is permitted, if necessary

- ✓ *for the transmission of the communication*
- ✓ *to maintain or restore the security of electronic communications networks and services*
- ✓ *to detect technical faults and/or errors in the transmission of electronic communications*

Article 6.2:

Processing of electronic communications **content** is permitted, if:

- ✓ *necessary for the provision of specific services for which the end-user has given his consent, provided that the purpose(s) concerned could not be fulfilled by processing information that is made anonymous*
- ✓ *all end-users concerned have given their consent to the processing of the content for one or more specified purposes that cannot be fulfilled by processing information that is made anonymous , and the provider has consulted the supervisory authority*

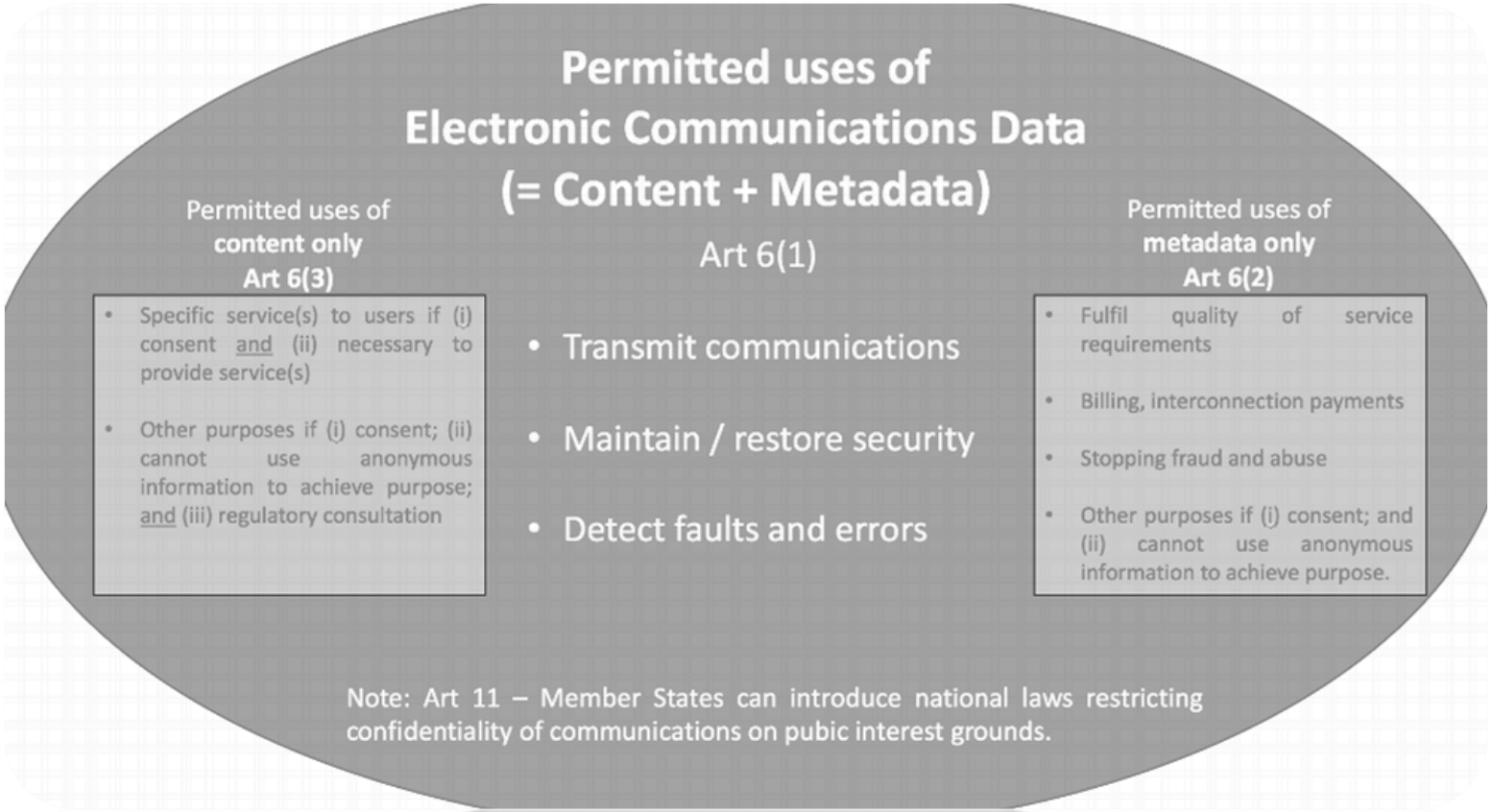
Permitted Processing of Electronic Communications Data

Article 6.3:

Processing of electronic communications **metadata** is permitted, if necessary

- ✓ *to meet mandatory quality of service requirements*
- ✓ *for billing, calculating interconnection payments, detecting or stopping fraudulent, or abusive use of, or subscription to, ECS*
- ✓ *for the provision of specific services or other specified purposes for which the end-user(s) has/have given his consent, provided that the purpose(s) concerned could not be fulfilled by processing information that is made anonymous*

Permitted Processing of Electronic Communications Data



New Business Opportunities

Once users have given their **consent** to process communication content and/or metadata, **traditional** **telecommunications** service providers will have **more opportunities** to use data and **provide additional services** (e.g. producing heat maps indicating people's presence)

Storage and Erasure of Electronic Communications Data

Article 7:

1. ECS providers shall erase electronic communications content or make that data anonymous, after receipt of electronic communication content by the intended recipient or recipients.

- ✓ *Such data may be recorded or stored by the end-users or by a third party entrusted by them to record, store or otherwise process such data, in accordance with the GDPR*

2-3. ECS providers shall erase electronic communications metadata or make that data anonymous,

- ✓ *when the data are no longer needed for the purpose of the transmission of a communication*
- ✓ *for billing purposes, after the period during which a bill may lawfully be challenged or a payment may be pursued in accordance with national law (if the data was processed for billing purposes)*

Consent

When is 'CONSENT' considered to be validly given?

- "Consent" has the same meaning as under the GDPR, i.e. freely given, specific, informed, active and unambiguous consent expressed by a statement or clear affirmative action.

- However, in the context of cookies, such consent may be expressed by browser settings and the Regulation places specific obligations on browser providers to ensure that appropriate consent settings and options are given to individuals.

- Consent can be withdrawn at any time, but service providers must remind end-users every six months that they have the right to opt-out.

Simpler rules on cookies

Under the Directive:

an overload of consent requests of each website separately for internet users

Under the proposed Regulation:

Refusal or acceptance via browser settings (Art. 10)

No consent required for non-intrusive cookies

- for “configuration purposes” (i.e. technically necessary or to keep your shopping cart history);
- providing a requested service;
- measuring the number of visitors to a specific website.

Full transparency without having to click on a cookie banners when visiting a website

astrea

Simpler rules on cookies

Article 8.1:
The use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware, other than by the end-user concerned shall only be allowed, if

- ✓ *the end-user has given his or her consent*
- ✓ *necessary for the sole purpose of carrying out the transmission of an electronic communication*
- ✓ *necessary for providing a requested information society service (e.g. add things to shopping cart)*
- ✓ *necessary for web audience measuring (provided that such measurement is carried out by the provider of the information society service requested by the end-user)*

Simpler rules on cookies

Article 8.2:
The collection of information emitted by terminal equipment to enable it to connect to another device and, or to network equipment is only permitted, if

- ✓ *it is done exclusively for establishing a connection; or*
- ✓ *a clear and prominent notice is displayed informing of, at least, the modalities of the collection, its purpose, the person responsible for it and the other information required under Article 13 GDPR (in case personal data are collected), as well as any measure the end-user of the terminal equipment can take to stop or minimise the collection, and only if the application of appropriate technical and organizational measures to ensure a level of security appropriate to the risks, as set out in Article 32 GDPR have been applied*

astrea

Simpler rules on cookies

- **Article 10.1***:*
  "Software placed on the market permitting electronic communications, including the retrieval and presentation of information on the internet, shall offer the option to prevent third parties from storing information on the terminal equipment of an end-user or processing information already stored on that equipment."

- Software installed before 25 May 2018 would need to offer the option to block third party cookies on the first update of the software, and at the latest by 25 August 2018.

- **Article 10.2:**
  "Upon installation, the software shall inform the end-user about the privacy settings options and, to continue with the installation, require the end-user to consent to a setting."

- Users should be offered user-friendly 'choice' from a set of privacy setting options, ranging from higher (e.g. never accept cookies) to lower (e.g. always accept cookies).

- Not dissuade users from selecting these higher privacy settings.

Protection against Spam

Under the Directive:

- Article 13.1, which prohibits the use of automated calling and communication systems, fax and e-mail for direct marketing without the prior consent of the subscriber or user.
- Strict interpretation leaving direct marketing by information society services such as Facebook, LinkedIn, Skype or Twitter unregulated.

Protection against Spam

Under the proposed Regulation:

- "any form of advertising sent to one or more identified or identifiable end users of electronic communications services"

  Regardless of the technology used, consent is needed for unsolicited commercial communications (**opt-in**) save where an individual's contact details have been obtained in the context of a sale (**opt-out**)

  Also protection against marketing phone calls **by default**, or by means of a right to object to the reception of voice-to-voice marketing calls, e.g. by registering on a **list** (corporate end-users)

- Marketing callers will need to display their phone number or use a **special prefix number** that indicates a marketing call.

Protection against Spam

Under the proposed Regulation:

- Important Distinction:

  - B2C communications: the sender of the communication has to obtain the consent of individuals for direct e-marketing purposes.

  - B2B communications: less protection: Member States must ensure that the legitimate interest of corporate end-users are sufficiently protected from unsolicited communications (by default or right to object, see *supra*)

Protection against Spam

Publicly Available Directories:

- **Natural persons**' data can be included in a **publicly available directory** on the basis of **consent**
- Publicly available directories inform about **search functions** and obtain natural persons' consent before enabling them
- **Legal persons** are given the **possibility to object** to being included in a publicly available directory

Harmonization & Enforcement

Updating the current Directive with a directly applicable Regulation aims to guarantee the same level of protection for all people and businesses as ECS providers will all be subject to **one single set of rules** across the EU (no need for national implementation as with the ePrivacy Directive)

Harmonization & Enforcement

under the Directive:

enforcement of implemented ePrivacy rules is regulated by each Member State individually

under the proposed Regulation:

ePrivacy rules will be enforced by the independent EU data protection authorities (already in place for the enforcement of the GDPR) . The one-stop-shop principle ensures uniform application across the EU.

astrea

Increased Fines

The proposed ePrivacy Regulation mirrors the fines in the new GDPR.

Infringements of the following rules could result in administrative fines of, the higher of 10,000,000 EUR, or up to 2% of the total worldwide annual turnover:
- "cookie" information and consent rules
- privacy by design obligations
- rules on unsolicited communications (i.e. failure to respect opt-in rules) and
- provisions on publicly available directories

Infringements of the following would be subject to administrative fines of, the higher of 20,000,000 EUR, or up to 4% of the total worldwide annual turnover:
- the principle of confidentiality of communications
- unlawful processing of electronic communications data and
- time limits for erasure

Right to sue for damages

Entry into Force

- Aim is 25 May 2018, together with the entry into force of the GDPR

- Far-reaching, detailed rules
  => difficult to achieve political consensus? Lengthy legislative process?

astrea

RECAP:
Benefits for Citizens and Businesses

- **Updated rules reflecting technological developments**: protection of confidentiality of communications across the EU, irrespective of the technology used.
- Directive => Regulation**: one single set of rules across the EU** which may lead to more legal certainty and less compliance costs for multinationals
- Consistency with the GDPR
- Clearer rules on 'cookies': **users will enjoy full transparency** without having to click on a banner asking for their consent on cookies each time they visit a website (although given stricter consent requirements even with browser level consent controls cookie banners are unlikely to disappear).
- Traditional telecommunications operations will have **more opportunities to process communication content and/or metadata to provide additional services** and to develop their businesses.
- Users will get **more control over spam and marketing phone calls**.

Criticisms and questions

Criticisms and questions

1. **What happens with data after the withdrawal of the consent?**

After withdrawal of the consent the processing of the data will stop, but should all stored data be erased too?

Criticisms and questions

2. Is "web audience measuring" (e.g. counting the number of views on a website) an acceptable exception? Do cookies used for analytics fall under the exception of "web audience measuring"? And what about third-party analytics cookies?

- Measuring tools from the same large firms => better safeguards needed

- Article 8(1)(d) explicitly provides that no consent is required for cookies if they are necessary for "web audience measuring", provided that such measurement is "carried out by the provider of the service requested by the user".

- However, it is not clear what "web audience measuring" exactly encompasses and whether third-party analytics cookies also fall under this exception.

Criticisms and questions

3. **Will browsers settings providing for the option to prevent the storage and processing of the information on the end-user's terminal be workable for website browsers?**

This proposed rule implies that there has to be some degree of communication between the browser and the publisher with regard to the refusal or acceptance of cookies by the end-user. However, the majority of websites still do not recognize Do-Not-Track signals.

Criticisms and questions

4. **Will web browsers settings providing for an option for users to reject third party cookies rather than a rule to provide a "reject all cookies" by default be efficient?**

There is no requirement that third party cookies, which are the backbone of the targeted advertising industry, should be blocked by default. Rather than requiring that the software is set to "do not track" mode, the official proposal **only requires that it *offers an option* to do so.** (< strong lobbying of advertising industry)

Criticisms and questions

5. **Although users may protect themselves through their browser settings, websites may still ask for consent. Sometimes they require either consenting or paying for the service. Is this acceptable?**

- Consent or monetary payment = consent as compensation for a (free) service.

- IF the service in question could be provided without advertising and IF declining entails that the service must charge money, can consent be considered to be freely given? Is the consent valid in this case?

Criticisms and questions

6. What about adblockers?

- The use of adblockers is not regulated

- The proposal allows website providers to check if the end-user's device is able to receive their content, including advertisement, without obtaining the end-user's consent

- If a website provider notes that not all content can be received by the end-user, it is up to the website provider to respond appropriately (for instance asking to switch it off to receive all website content)

Criticisms and questions

7. Do the new rules mean publishers cannot advertise anymore, considering the general 'Do Not Track' option in the browser settings?

- In order not to dry out an important source of finance for the free internet, the "privacy by design element" must be applied with caution

- Websites relying on cookies for market and tracking purposes will continue to want to obtain opt-in consent to override the general 'Do Not Track' option
  (-> still pop up consent boxes)

Criticisms and questions

8. Does the Proposal jeopardize directories and individual entrepreneurship?

- Shifting the burden of getting consent from telcos to directory providers (Article 15)
- Reducing the possibilities of free online presence for individual entrepreneurs
- Lowering the access to financing possibilities for individual entrepreneurs
- Responsibility of ECS providers to obtain content ?
- Unfair competition ?

Criticisms and questions

9. What about the harmonization of the data retention rules in the proposed Regulation?

Right to limit confidentiality of communications of citizens to safeguard one or more of the 'general public interests'

- cf. Article 23(1) GDPR
- jurisprudence of the CJEU - *legality, necessity and proportionality* (cf. Joined Cases C-203/15 *Tele2 Sverige AB v Post-och telestyrelsen* and C-698/15 *Secretary of State for the Home Department v Tom Watson and Others)*

=> *De facto* no harmonization of data retention rules due to considerations of national security, which remains a competence of the Member States within certain boundaries!

Criticisms and questions

10. How should end-users and consumers be informed about 'tracking' in public spaces (Art 8(2) b)?

Retail stores are using technology to track your movements around the store. Based on the information they collect, visitors might receive an email with a personalized offer.

How to inform your customers?

- big sign with the following text: "Tracking going on! Switch off your phone if you do not agree with it." (Note: simply disabling wi-fi connection does not prevent tracking.)
- Should Wi-Fi tracking be made that easy?
- Should stores be allowed to get away with simply hanging up a poster?

Is this tracking of people by default, especially in public places, acceptable??

Criticisms and questions

11. Does the Regulation provide sufficient safeguards against cyber security risks?

- Unlike the Directive, no cyber security obligations!
- Should some standard for end-to-end encryption be included in the ePrivacy Regulation ?
- Recital 37: appropriate protection measures
- EU Parliament may demand for stricter cyber security obligations

Criticisms and questions

12. Should there be a collective redress mechanism?

- No reference to the corresponding Article 80 of the GDPR?!

- Omission of an important new mechanism to uphold data subjects' rights
  (-> rebalancing the power between large companies and individuals)

- Collective redress was included in the leaked version of December (strong lobbying?!)

Criticisms and questions

13. Are both the GDPR and the ePrivacy Regulation necessary?

- Electronic communications need a special regime due emergence of new technologies

- Article 7: right to respect for private and family life, home **and communications**

- Not only individuals but also businesses

Criticisms and questions

14. Is there a potential overlap with the GDPR?

E.g. processing personal data contained in electronic communications, or how to process cookie data that qualify as personal data

=> both the ePrivacy Regulation and the GDPR will apply.

CONCLUSION

- Overhaul of ePrivacy Directive is necessary and overdue

- Commission identified key issues but final text came out weaker than some had hoped for it to guarantee confidentiality and privacy of communications of EU citizens and to actually reduce cookie pop-ups and banners

- Still ePrivacy Regulation is set to have a major impact on companies (implementing browers options, higher consent levels) and the latter should review their online practices and monitor the legislative process closely

- A lot of thorough work is still required to secure balance between consumer interests and achieve a consistent approach

astrea

CONTACT

Steven De Schrijver
Partner, Astrea
Brussels (Belgium)

T: +32 2 215 97 58
E: sds@astrealaw.be
W: www.astrealaw.be