FACTSHEET ePrivacy

What does ePrivacy stand for?

The respect of our privacy is an established right under the EU Charter of Fundamental Rights. A person's private life, home and correspondence must be respected. Basically, it is forbidden that someone enters your home without your permission, that your conversations at the kitchen table are snooped on or that somebody opens a letter addressed to you. ePrivacy is about the same things but related to the online world and electronic communications. This includes phone calls, emails and surfing on the internet.

Why does the EU's ePrivacy law require a facelift?

The current ePrivacy dates from 2002 and was last updated in 2009. That is a long time ago in terms of digital developments. In recent years, instant messaging services such as WhatsApp, Messenger and Telegram and internet calls via for instance Skype have fundamentally changed the way we communicate with each other. Yet, the communications running through these 'novel' communications services are not protected in the same way as with a regular SMS or phone call.

That is one of the reasons why in January 2017, the European Commission has proposed a Regulation on Privacy and Electronic Communications to replace the e-Privacy Directive.

9 out of 10 respondents to a recent survey say that it is important that the information on their computers can only be accessed with their permission.

Eurobarometer 2016.

The EU just adopted a data protection law. Why is the ePrivacy law still needed?

In May 2018, the EU's new data protection rulebook will enter into force. Data protection and protection of one's privacy are closely related but far from the same. The fact is that we are talking about two distinct fundamental rights under the EU Charter. Data protection is about our right to control the use of our personal information and to protect us from abuses. The right to privacy is about the right of the individual to define what is private. It's for example about having the right to read your newspaper without anyone looking over your shoulder, or having a private conversation with a friend without anyone listening to what you are saying. Consumers' private spheres and communications should be respected regardless if personal data are involved.

The e-Privacy Regulation brings an additional layer of protection: it would protect the confidentiality of communications and shelter consumers from online tracking and unsolicited commercial communications.

Tracking – the risk and how to fix it

People are constantly tracked when they are online. Whenever you visit a website or open an app, multiple companies collect information about what you read, which links you click on and what topics you're interested in.

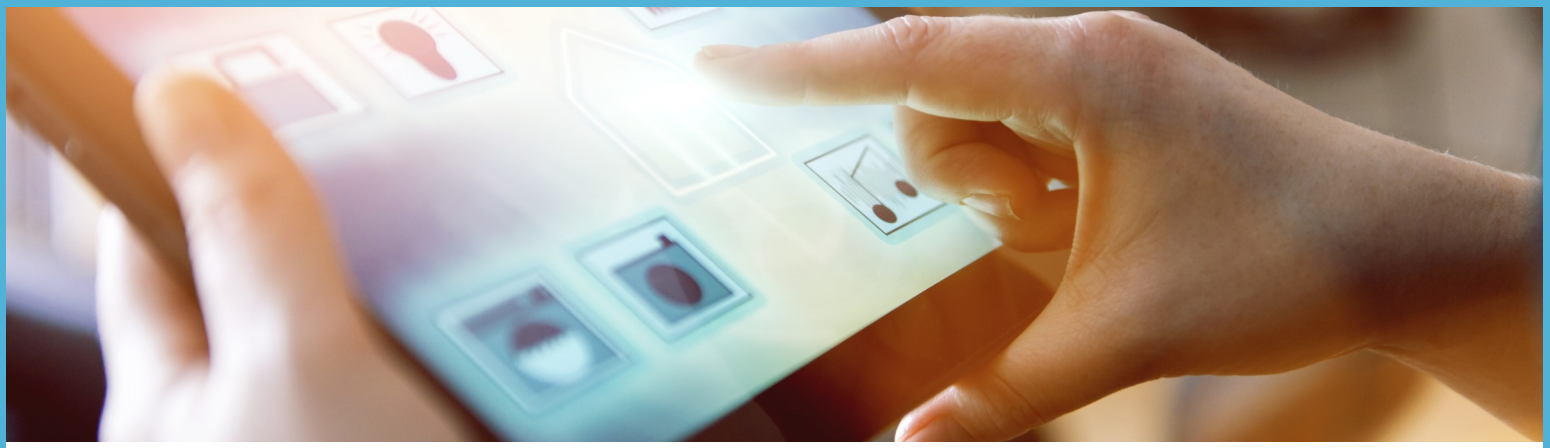
89% of consumers agree that the default setting of their browser should stop their information from being shared.

Eurobarometer 2016.

BEUC The European Consumer Organisation

Rue d'Arlon 80
B-1040 Brussels
Tel +32 (0)2 743 15 90
www.beuc.eu

This factsheet is part of an activity which has received funding under an operating grant from the European Union's Consumer Programme (2014-2020).



Companies utilise the information they gather to build user profiles, which are traded online and used to deliver behaviourally targeted advertising. These profiles could also be used to discriminate consumers and influence their behaviour. For instance, an insurance company could decide not to insure a person if their user profile shows that they frequently visited a website selling whiskey.

We believe online tracking should only happen when consumers give their consent and would like that the default rule is that consumers should not be tracked. So-called 'tracking walls', which force a consumer to accept being tracked in exchange for access to a website, notably for behaviourally targeted advertising purposes, should be forbidden. Basically, consumers should have the possibility to use online services without being under constant commercial surveillance.

Privacy by default

Put simply, privacy by default would make that the settings of any hardware or software are configured to provide the highest level of privacy protection from the outset. Consumers often do not have the knowledge to distinguish between different privacy settings – which too often are explained in overly complex terms and presented in a way that lure the consumer into accepting settings that undermine his/her privacy.

Recommendations

Privacy by default and strong safeguards against tracking are two core demands but more needs to happen to ensure consumers are protected when using online services:

- The **confidentiality of communications** must be guaranteed in all types of electronic communications services, including when the communications service is only a secondary feature (e.g. a messaging function in an online game).
- As a rule, **communications services providers should not use the content of their users' communications** and its associated metadata beyond what is necessary to deliver the service without their consent. Only very limited exceptions to this rule should be allowed, focused on purely technical and administrative purposes and only when the processing of the communications data is strictly necessary for the purpose in question.
- **Companies should not be allowed to claim 'legitimate interests'** to process user's communications data. This could lead to abuse by companies claiming for instance that processing communications data for targeted advertising would be a legitimate interest.
- **Consumer groups (and other representative organisations) should be allowed to bring forward legal actions** – on behalf of consumers or the public interest – when the rules on e-Privacy are breached.