Privacy signals: A simple guide

EDRi
European Digital Rights

What is a privacy signal?

A privacy signal is a tool that automatically tells websites, apps and connected devices **what you have decided about tracking and data use.** For example, it can say: 'do not track me', or 'I consent to this specific use of my data'.

The signal is machine-readable. This means it is sent in a format that websites, apps, devices and other systems can understand automatically, **without asking you the same question again and again.**

You make your decision once. Your browser, operating system, app, or another privacy tool sends it automatically. Websites, apps and connected devices receive it and must respect it.

You remain in control. You can change your choices at any time. Instead of answering the same question on every website, your choices travel with you. Privacy signals are about making rights usable. A right that requires people to fight through confusing banners, hidden settings, or device-by-device menus is not effective in practice.

Why are we discussing privacy signals now?

In November 2025, the European Commission proposed changes to the EU digital rulebook, known as the **Digital Omnibus.** Many of these changes would **reduce core protections** for people using or accessing the internet by allowing more data use, weakening safeguards, and putting more responsibility on individuals to manage their rights. However, one change goes in the opposite direction: privacy signals.

This matters because **many websites and apps try to collect large amounts of data about people,** including through cookies, trackers, and advertising technologies. This data can be used to profile people, target them, shape what they see online, and expose them to manipulation, discrimination or exploitation.

People are already trying to protect themselves. EU survey data shows that many people change browser privacy settings, use tools to block ads or monitoring, avoid websites because they worry about tracking, or refuse the use of their data for advertising. According to 2025 Eurostat numbers, 76.9% of EU internet users took steps to manage access to their personal data in 2025. While as per a 2016 Eurobarometer, 89% of respondents in an EU survey agreed that browser default settings should

stop their information from being shared, and 82% said tools for monitoring their online activities, such as cookies, should only be used with their permission. This shows that demand already exists. The problem is that we currently have to fight service by service, setting by setting, banner by banner.

A new proposal (Article 88b of the GDPR) would **introduce the possibility for us all to express consent and other privacy decisions automatically**, for example through their browser or phone, and have these choices respected by websites and apps.

In practice, you could choose 'I do not want to be tracked', or consent to specific uses of your data, without clicking through repetitive cookie and consent banners on every website. **Services would have to respect that choice.** If properly designed and implemented, this could make privacy much simpler and more meaningful: it can reduce 'cookie fatigue', simplify compliance, and restore control back to individuals.

This is why privacy signals are the only aspect of the proposed Digital Omnibus that could genuinely simplify our ability to exercise their fundamental rights.

Why should anyone care?

We all have realised that **the current system does not work for people.** Too often, it makes refusal harder than acceptance, turns privacy choices into confusing interfaces, and asks users the same question again and again until many simply give in.

Think how many times you see cookie banners in a day. Many are designed to push you towards 'accept'. Some hide refusal behind extra clicks, long lists of toggles, unclear categories, or references to hundreds of third parties. Many of us click 'accept' without reading the conditions because we want to access the website quickly. That is **not meaningful control, it is friction and it is by design.** It makes it as hard as possible for you to have genuine control and autonomy over your digital life.

Privacy signals could change that. They would allow people to express their wishes once, change them whenever they want, and have them respected automatically across services. This reduces banner fatigue, limits manipulative design, and makes rights more realistic in everyday life.

It's not only people who will benefit for being able to make more mean-

ingful choices. Smaller services and public authorities would also benefit. A system based on repeated banners is expensive, fragmented, and difficult to enforce. **A system based on machine-readable decisions would make the rules easier to apply, easier** to audit, and easier for authorities to enforce at scale

What the current debate gets wrong

Some, particularly within industry, argue that privacy signals will create confusion, weaken consent, or break the internet economy. These claims misrepresent both the current system and what signals actually do.

Confusion already exists today. It is produced by repeated banners, inconsistent interfaces, and design practices that push people to accept. **Consent is already weak in practice.** Clicking through dozens of prompts does not create meaningful, informed choices.

Signals do not remove control, but rather they make it more 'usable' in practice. They let people set explicit choices in a clear environment, change them at any time and avoid being asked the same question over and over again.

What the debate gets wrong is not whether signals are perfect, but whether the current system should continue to exist as it is.

Do privacy signals weaken consent?

No. This question matters because some industry actors argue that automated signals would make consent less clear. The opposite is true if the law is well designed.

Today, consent often happens through banners that make refusal harder than acceptance. Sometimes people face long lists of toggles, hidden options, and confusing categories. This does not support meaningful consent. **It turns the exercise of rights into a burden.**

A privacy signal does the opposite, and can make consent more meaningful. It **allows a person to express a decision once, through a clearer and more consistent interface, and to change it at any time.** A well-designed signal can also reflect different types of choices. For example, a person can refuse tracking for behavioural advertising while consenting to a specific use of data by a service they trust. This is much closer to the

GDPR requirement of freely-given, specific and informed consent than the current banner model.

Signals are sometimes presented as a if they had to be a single 'yes' or 'no' setting. That is not true. Nothing prevents signals from expressing choices by purpose, by category of processing, or by context, reflecting the different nuances that the user want to see in their browsing experience. This would allow people to make more nuanced decisions without navigating a different banner on every website.

The risk is poor design. That is why the law must set clear requirements for how signals work.

Are privacy signals technically feasible?

Yes, the **technology already exists** and most of us already use similar tools. Browsers and other user tools on our devices already communicate choices automatically. For example, devices already remember language settings, accessibility choices, location permissions, notification permissions, and whether an app can access the camera or microphone. Privacy signals use the same basic logic. The difference is that they communicate decisions about tracking and data use in a machine-readable way.

Large technology companies and browser providers have already started restricting some forms of online tracking automatically in response to widespread concerns about privacy abuses and intrusive data collection. This shows that automated **privacy protections are already technically feasible.** The real question is whether people themselves should be able to decide how tracking is handled and have those choices respected across services.

What is missing are clear rules to make sure everyone respects these signals in the same way. That is why the law matters. Without legal effect, companies can ignore privacy signals, as many did with earlier tools such as 'Do Not Track'.

With legal effect, companies must respect people's decisions, and regulators can check whether they do so. This matters because today many websites, apps, advertisers, and data brokers benefit from collecting and sharing data even when people do not meaningfully agree. Privacy signals would change that incentive. They would make it harder to ignore people's choices and easier for regulators to check compliance.

Are privacy signals new?

No. The basic idea is not new.

EU law already points in this direction. The GDPR recognises that people can exercise the right to object by automated means. The ePrivacy Directive already allows choices to be expressed through browser settings. The EU rules on political advertising also recognise the role of automated signals.

For years, there have been efforts to allow people to communicate automatic privacy choices through browsers and other software. Some earlier attempts were too weak because they depended on voluntary compliance. Others were more advanced but they never received the necessary legal backing for wide adoption.

So what is new is not the concept, but the **opportunity to finally make them work** in practice in the EU.

Other jurisdictions are moving ahead. In California, for example, the law requires browsers to provide signals and services to respect them from 2027. This shows that privacy signals are possible and being put into practice.

The EU has long been seen as a global benchmark for privacy and data protection rules. **Without clear rules on privacy signals, the EU risks falling behind** in making digital rights effective in practice.

Whose interests do privacy signals protect?

Privacy signals protect people first of all. They help them express choices in a clear and practical way, without having to fight through banners and settings on every site.

They also **protect smaller services, publishers, and organisations** that need workable rules instead of endless consent pop-ups and expensive compliance layers. A better system should not reward those with the most aggressive interface design or the biggest compliance budget.

They also **protect the public interest.** Clear signals can support fairer competition, more consistent enforcement, and a digital environment in which rights are easier to exercise in practice.

Okay, but in practice: does this mean I do not have to click cookie banners every time?

Yes, the objective is to reduce them dramatically.

If your browser, operating system, or app already communicates your decision, there is no need to ask you the same question again. The website or app can read the signal and apply it.

You still remain in control. You can change your choice at any time.

Technically, what does a privacy signal actually do?

A privacy signal works before tracking starts. The signal is sent by your browser, operating system, app, or a privacy extension. It communicates your decision in a machine-readable way.

Any actor attempting to access your device (e.g. websites, apps, advertising partners, and so on) must read the signal and apply the choice.

It's important to stress that **signals do not remove context or explanation.** Services can still explain how they operate, including whether they rely on advertising, subscriptions, or other models. What changes is that **once a person has made a valid decision, the service cannot keep asking the same question** through repeated banners or prompts. Explanation is compatible with signals. Pressure is not.

In short, privacy signals can communicate different kinds of decisions:

- They can say 'yes' to specific uses:
  - 'I consent to this specific use of my data'
  - 'I allow this service to remember my choice'
  - 'I allow this feature because I asked for it'

- They can say 'no':
  - 'do not track me'
  - 'do not share my data with third parties'
  - 'do not profile me'
  - 'do not use my data for targeted advertising'

- They can also say 'I changed my mind':
  - 'I withdraw my consent'
  - 'I object to this processing'

This means that signals are not only about blocking. They can support consent, refusal, withdrawal, and objection.

The key difference is timing. The signal acts to prevent tracking before data about you are collected, not after the fact, when the harm may already have happened

Given all the above, who would benefit from the current banner system?

The current banner system mainly benefits parts of the **adtech ecosystem and large online services whose business models rely heavily on large-scale tracking and profiling** across websites and apps. It also benefits some consent management platforms and advertising intermediaries that have turned legal compliance into a confusing market of banners, pop-ups and consent tools.

Many small services are not the winners of this system. They often use complex consent banners because they have been told this is the safest way to comply, even when those tools are confusing for users and risky for the service itself.

Privacy signals would help change this. They would reduce reliance on banner infrastructure, make people's choices clearer, and make compliance easier for services that want to respect rights.

Is it true that privacy signals would harm publishers and advertising-funded services?

Some argue that privacy signals would undermine advertising-funded services, including independent media. This assumes that current consent practices are both lawful and sustainable. In reality, many rely on repetitive prompts and design choices that do not reflect meaningful user consent.

Privacy signals do not stop advertising. They let people consent to specific uses of their data, while also making it easier to refuse tracking, pro-

filing, and data sharing for targeted advertising. Advertising that does not rely on intrusive tracking, such as contextual advertising, can continue.

Privacy signals can actually create a fairer playing field. Today, services that invest in less intrusive models, clearer interfaces, or contextual advertising can be placed at a disadvantage compared with actors that collect more data, use more aggressive consent flows, or rely on complex adtech chains. A system that respects machine-readable choices would reward services that respect people's rights, rather than those with the most effective pressure tactics.

Many smaller publishers and services are not the winners of the current system. They often rely on complex consent management tools because they have been told this is the safest way to comply. Privacy signals could reduce that dependency and make compliance easier for services that want to respect rights.

Does this give too much power to browsers?

No. **Privacy signals do not require a single tool or provider,** as they can be implemented by:

- browsers;
- operating systems;
- apps;
- privacy tools like dedicated software or even browser extensions;
- enterprise devices;
- accessibility tools.

Users can choose which tool they use and they can change decisions at any time. This distributes control across different user agents rather than concentrating it in websites, rebalancing the power of users.

That said, **the law should also make sure that no single browser, operating system, or platform can control the meaning of the signal.** The user's decision must come first. Technical standards can help different tools work together, but they should not allow powerful companies to redefine or weaken people's rights.

Is this only about privacy and data protection?

Privacy signals are first and foremost about privacy, data protection, and the protection of devices against tracking. But the same idea can help

solve other digital harms too.

The basic idea is simple: people should be able to express important rights-based choices once, in a machine-readable way, and have digital services respect them automatically. This logic can support a safer and fairer digital environment beyond cookies and advertising tracking. For example, automated signals could help with:

- **Applying stronger GDPR protections, including for children.** Automated signals can help services apply existing data protection rules in practice. For example, they can communicate that profiling, behavioural advertising, or data sharing should not take place, or that only strictly necessary data should be used. This matters for everyone, and it is especially relevant where children are likely to use a service, because the GDPR recognises that children merit specific protection. This does not have to lead to the building of a separate internet only for children, or to expanding age checks across the web. Many safeguards, such as no behavioural advertising, no profiling based on vulnerabilities, safer defaults, and data minimisation, should protect society as a whole. Signals can help make those protections easier to apply without putting the burden on each person to fight every interface one by one.

- **Deceptive and addictive design.** Automated signals could help people say that they do not want personalised pressure, manipulative prompts, or design features that push them to spend more time or money than they intended. This would not replace strong legal bans on deceptive design, but it could make rights easier to exercise in practice.

- **Unfair personalisation.** Signals could help people refuse personalisation based on tracking, inferred vulnerabilities, emotional profiling, or behavioural surveillance. This is relevant because many people find these practices unfair. A recent survey found that only 19% considered it fair to target people with ads and content based on information about their lives, weaknesses and vulnerabilities, and only 16% considered it fair for a website or app to require access to information about them in order to monetise their behaviour.

- **Cybersecurity.** Data that is not collected, shared, or stored unnecessarily cannot leak, be stolen, or be abused later. Privacy signals can support data minimisation by reducing unnecessary collection and sharing. They are not a substitute for cybersecurity rules, but they help reduce the amount of data exposed to risk.

So privacy signals are not a magic solution for every digital harm. They must not replace strong bans, duties, and enforcement. But they can **become part of a wider rights infrastructure:** a practical way for people to express choices and protections once, and for services to respect them by design.

What must decision makers fix for signals to actually work?

The current proposal is a good start but it has gaps. At the moment, proposed the Article 88b of the GDPR would allow automated means to express consent, refuse consent, and exercise the right to object. But this is not enough.

For privacy signals to become a real solution, **the law should**

- include **withdrawal of consen**t;
- make signals **legally binding**;
- ensure signals **apply to all actors** involved in tracking and data sharing;
- **cover all** browsers, operating systems, apps and other privacy tools;
- guarantee that **signals cannot be overriden** by repeated banners or manipulative prompts;
- ensure signals **work from the start**, instead of being delayed for years while technical standards are developed.

These are key issues that need improvement for privacy signals to become a real solution.

Why do signals need to be legally binding?

This is what happened with earlier tools such as 'Do Not Track'. The technology existed, but services were not required to respect it. **Privacy signals will only work if the law gives them legal effect**. That means companies must respect the signal, and regulators can enforce the rule when they do not.

This is why legal clarity in Article 88b matters. This is not a technical question but a question of compliance.

Why is withdrawal important?

Under the GDPR, withdrawing consent must be as easy as giving it. Signals can make this real in practice.

If someone changes their mind, they **should be able to change their decision** once and have that decision applied across services.

Without withdrawal, signals would only covert the first moment of choice. They would not give people full control over what happens later.

Why Articles 88a and 88b must apply at the same time

Proposed Article 88a (Digital Omnibus) would expand situations where tracking may occur without consent by introducing exceptions to cookie consent rules. Article 88b introduces privacy signals to allow users to automatically refuse such tracking. These two changes are meant to operate together.

If exemptions expand first but signals come later, tracking increases before people have any new way to control it. The balance shifts in one direction only.

Imagine certain analytics become allowed without consent. If signals are not yet operational, the user has no effective way to object. **Tracking happens by default, and this is why timing matters.**

Why privacy signals should sit under ePrivacy

Privacy signals should be about access to devices and tracking technologies, not only about cookies on websites. Tracking can happen through browsers, apps, software development kits, smart TVs, connected cars, wearables, toys, speakers, and other connected devices.

This is exactly what ePrivacy regulates, even if many stakeholders keep arguing for getting rid of the law. **ePrivacy applies at the moment someone tries to access your device and that's when privacy signals operate too.** They say yes or no before tracking begins.

This is also why the debate should not be reduced to 'cookie banners'. Cookie banners are one visible symptom of the problem, but the real issue is wider: **who gets to access your device, collect information from it, and use that access to monitor, profile, or influence you.**

The Commission proposes to place privacy signals in the GDPR. This shifts them into a different logic. The GDPR mainly regulates what happens once personal data is processed. ePrivacy regulates the earlier

moment of access to a device. Signals therefore risk becoming simply another consent layer instead of a tool that prevents tracking and genuinely protects people's rights online.

Putting privacy signals under ePrivacy keeps their preventive function. It ensures they **stop tracking before it starts, not afterwards.** Privacy signals should be regulated under Article 5(3) of the ePrivacy Directive because they operate at the moment of access to a device. This should cover websites, apps, connected devices, embedded third-party tools, and other technologies that store or access information on terminal equipment.

At the same time, the law should clarify that when another EU rule, including ePrivacy, relies on consent as defined by the GDPR, a valid automated signal can express that consent, refusal, withdrawal, or objection. This **avoids a gap between ePrivacy and GDPR.**

In practice, this means: ePrivacy decides when a signal must be respected before tracking starts. GDPR decides whether any consent expressed through that signal is valid, specific, informed, freely given, and easy to withdraw.

Press enquiries
press@edri.org

Brussels office
brussels@edri.org

Phone number
+32 2 274 25 70

Visit us

Rue Belliard 12
1040 Brussels
Belgium

Follow us

Mastodon
Facebook
LinkedIn
Youtube
Instagram

EDRi
European Digital Rights