AK EUROPA

Position Paper
December 2019
Consumers

Regulation concerning the respect for private life and the protection of personal data in electronic communications:

The digital private sphere requires better protection!

COM (2017) 10 final

The AK's position

Safeguarding a high level of consumer protection and developing sectoral data privacy laws in Europe is one of our major concerns. Therefore, we place special emphasis upon ensuring that the needs of telecom and internet users, regarding the adequately strict protection of their privacy and personal data, receive appropriate attention.

"Over-the-top" surveillance

Consumers live in a densely networked environment. If you use electronic communications, you inevitably leave traces behind: the list of numbers called from your mobile phone, data traffic stored by your mobile network operator for invoicing purposes and anonymised location analyses, cookies in web browsers, access protocols on web servers, the mail server protocol at your internet service provider (ISP), your user profile at your smart home service provider, etc. Geodata from smartphones can even provide sensitive information: whether someone regularly goes to a hospital or visits a religious institution. Seemingly harmless (acceleration) sensor data can also reveal whether someone is at work, at home or driving their car at the time. The storage and utilisation of such data impinge on the private sphere.

Every point of contact with smart devices leaves personal data traces behind. These can be used to create detailed individual use and location profiles or, no less controversially, assign people to groups using pseudonyms or anonymised data according to certain behavioural patterns or project future behaviour. The interfaces with the internet, where consumer behaviour can be observed, stored, evaluated and transferred to third parties, give a uniquely exact picture of what we do, not do, think, who we have contact with, and much more.

Background

The proposal published by the EU Commission in 2017 intends to replace the previous e-Privacy Directive. Article 1 of the new Regulation defines its aim as the protection of fundamental rights and freedoms of the individual when using electronic communication services. The guiding maxim is the right of internet users to a private sphere, data privacy and confidentiality of communication. At first glance, this sounds promising, particularly since a 2015 Eurobarometer survey revealed the major concerns of consumers regarding their digital rights: 78% think that online service providers have too much customer data; 73% always want to be asked for their explicit consent. Years later and with numerous additional examples (such as data abuse by Facebook/ Cambridge Analytica), the mood has scarcely changed.

Summary of the criticism

Recent discussions in the Council do not satisfy the expectations of consumers. On the contrary: the revised passages promote free data flows within Europe.

- **To date** the metadata held by telecoms and internet providers (such as location or connection time of consumers) could only be used to establish the connection, ensure network security, for invoicing and – subject to the user's consent – for their own marketing purposes and additional services.

- **In the future** companies as well as scientific and research organisations, which have direct – or, by purchasing anonymised data, indirect – access to metadata, would be able to use metadata for numerous purposes, often without the consent of the individual and – if pseudonymised – for an unlimited period of time. Companies can access end devices without the consent of consumers via cookies and other methods for vaguely defined purposes such as security, fraud recognition or statistical counts. However, the obligation of browser developers to at least offer privacy setting options has been removed all together. The reason, far from safeguarding fundamental rights, is that it is advantageous for US browser developers.

- **Outlook**: The most recent discussions have abandoned the objective of protecting fundamental rights and aim at boosting the growth of the digital industry. The digital economy and science or research linked to business interests hope to exhaust the options offered by data-driven business models much further. Lowering the bar for the use of metadata and access to end devices is seen as an obstacle, for example, to the lucrative activity of spying on the behaviour of internet users via cookie walls (in return for the offered online content), the physical tracking of people's movements via the mobile phone in their pockets, e.g. in shops or shopping malls, the commercial exploitation of big data which smart devices generate en masse, or the need for additional training data to develop artificial intelligence.

- **What consumers want**: People are highly dependent on electronic communication in their daily lives. Yet, consumers are left with little choice. They have to submit to the conditions of operators, which they do not really agree with so that they can participate in digital life. Without a commitment to the strict protection of fundamental rights in the e-Privacy Regulation, which must also include clear precepts and prohibitions, users of smartphones, PCs, smart cars and heating systems, etc., will not be able to exercise self-determination over their data and their private sphere. With regard to the concern of consumers quoted at the start of this text ("providers collect far too much data online"; "we always want to be asked for our consent to our data being used") the right to self-determination and the principle of data minimisation should, in fact, be strengthened instead of continually weakened.

- **The red line**: The Commission's proposal of 2017 extended the scope for the commercial usage of data compared to the protection, which European citizens still enjoy in accordance with Directive 2002/58/EC. It is not acceptable to further weaken the standards of protection.

Therefore, consumer protection organisations demand: The digital private sphere requires better protection!

What needs to change

No commercialisation of metadata without consumers' consent

The consent of those affected must be obtained without exception for any data use purposes which are not essential for the provision of the service. The use of metadata for other "compatible" purposes must be prohibited without the consent of those affected (a solely right of objection is not enough). The use of data to identify abuse by users is too vague and can always be claimed in order to avoid having to immediately delete or anonymise data. Data usage for statistical or scientific purposes (in an encrypted or pseudonymised form) is also unthinkable without the consent of the consumer. When processing data of specific public interest the approval of the data protection agency may replace individual consent.

Moreover, the exploitability of metadata will in future exceed levels seen until now (network security, fee billing, marketing of communications services or provision of services with added value, each with prior consent of the user). The EU Commission acknowledges that users "want to control the use of electronic communications data for purposes other than conveying the communication" (Recital 17). Therefore, the consent of those affected must always be obtained for other purposes. Without the consent of those affected, the use of metadata for purposes "compatible" with the original purpose should be prohibited. Consent should also be obtained for statistical or scientific use because the use of pseudonymised data (which, in fact, can be traced back to the individual) is an infringement of fundamental rights. Even the assignment to anonymised groups based on behavioural characteristics can have negative consequences for consumers (behavioural control, manipulation, discrimination, etc.). However, in line with the demands of the online industry, an explicit right to object would not be enshrined in the Regulation.

E-Privacy comes down to "Do not track!"

Compulsory strict default settings for hardware and software: The Regulation must state specifically how mobile phones and web browsers are to be pre-set to minimise data collection.

Those tasked with protecting consumers and data across Europe are complaining that effective protection against one of the biggest threats to privacy is lacking: the spying on internet users' behaviour. Data analysts outperform themselves by using algorithmic evaluation of surfing behaviour: Be it through the classification of individuals according to their characteristics and preferences or through predictions of their future behaviour, access to the end devices of users and mining the data extracted from the devices using analytical tools signifies profits for internet companies and the loss of privacy for those concerned.

Cookies (and other tools) are used to investigate people's surfing behaviour. According to the draft Regulation, any use of the "processing and storage capabilities" of end devices is expressly prohibited (subject to extensive exceptions) unless carried out by the end-user concerned. The General Data Protection Regulation regulates technical data protection "by default" (the strictest possible presetting for devices and software). This provision must be clarified in the Regulation, otherwise, it will remain dead letter. Consent to access end devices can also be obtained through the browser settings selected by the user. "Do Not Track" is the name of a web technology that is offered as an option in modern browsers. If activated by the user, websites visited are automatically notified that the user objects to data being stored or to a user profile being created. However, according to the draft Regulation, browsers do not have to be pre-set to the highest privacy setting. Users should merely be offered a number of optional settings. Article 10, which contained this instruction, was deleted without substitution. A Eurobarometer survey by the EU Commission in 2016 revealed that around 40% of Austrian respondents did not know how to change their browser settings. Higher levels of privacy in default settings would help those with fewer digital expertise.

No to "tracking services": No access to end devices for the purposes of statistical counting and no physical surveillance by "tracking services" without the consent of those affected

Recent discussions also open up a gateway to surveilling consumers in their offline everyday life. Shops, which identify their customers (via their smartphones and WLAN or Bluetooth connections) and wish to track their movements or durations of stay, would not even have to seek their consent. A simple notice – for example in the shop – is considered to be sufficient. Tellingly, the scanning of device-related information is referred to as a "tracking service" for the purpose of people counting, providing data on the number of people waiting in line, placing personalised ads or tracking individuals over time.

In the future such offline tracking shall occur without the consumer's consent. Consumers shall merely be informed by a notice that they are entering a monitored area. Only the notice would inform on the purpose and range of the tracking, the person responsible for it and existing measures for the user to stop or minimise the data collection. 54% of consumers surveyed by the Federation of German Consumer Organisations (VZBV) categorically refuse such personal tracking. They see an explicit ban as the only adequate response to this development. The data usages are, in the opinion of AK, unthinkable without the consent of those affected.

No access to end devices without the consent of users in order to identify technical errors or fraud

This right of access is too extensive and could be misused for illegal data usage. The requirement to obtain effective consent would at least ensure that consumers are actually informed of all details of processing (what for, on what legal basis, to what extent, how long, etc.). Only in this way can those affected challenge excessive access and not themselves fall victims to non-transparent data use and abuse.

Contact us!

In Vienna:

Daniela Zimmer
T +43 (0) 1 501 651 2722
daniela.zimmer@akwien.at

Bundesarbeitskammer Österreich
Prinz-Eugen-Straße 20-22
1040 Vienna, Austria
T +43 (0) 1 501 65-0

www.arbeiterkammer.at

In Brussels:

Peter Hilpold
T +32 (0) 2 230 62 54
peter.hilpold@akeuropa.eu

AK EUROPA
Permanent Representation of Austria to the EU
Avenue de Cortenbergh 30
1040 Brussels, Belgium
T +32 (0) 2 230 62 54

www.akeuropa.eu

About us

The Austrian Federal Chamber of Labour (AK) is by law representing the interests of about 3.8 million employees and consumers in Austria. It acts for the interests of its members in fields of social-, educational-, economical-, and consumer issues both on the national and on the EU-level in Brussels. Furthermore the Austrian Federal Chamber of Labour is a part of the Austrian social partnership. The Austrian Federal Chamber of Labour is registered at the EU Transparency Register under the number 23869471911-54.

The main objectivs of the 1991 established AK EUROPA Office in Brussels are the representation of AK vis-à-vis the European Institutions and interest groups, the monitoring of EU policies and to transfer relevant Inforamtion from Brussels to Austria, as well as to lobby the in Austria developed expertise and positions of the Austrian Federal Chamber of Labour in Brussels.