ePRIVACY REGULATION – BETTER PROTECTION FOR PRIVACY

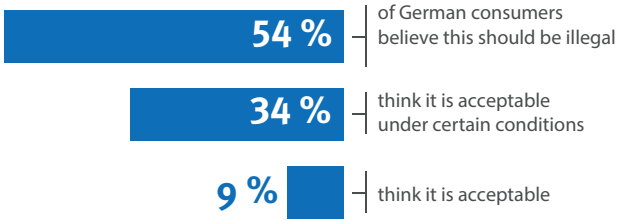
More and more people are using information society services like Skype, WhatsApp and Facebook in their everyday communication. Unlike traditional communication channels such as the telephone and text messages, information society services are frequently not covered by current telecommunications legislation. This means that confidential communication and personal data is not protected by law. The EU's new ePrivacy Regulation is set to change that.

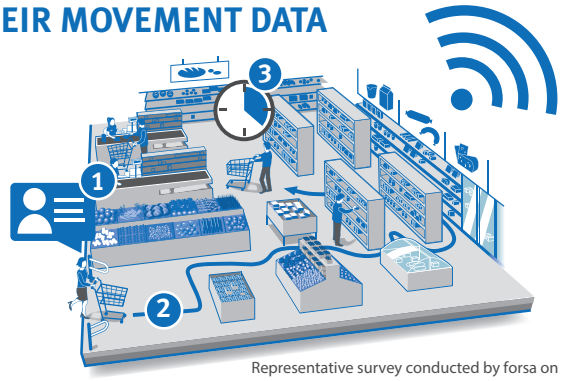
Since 2002, the protection of personal data and privacy in electronic communication has been governed by the ePrivacy Directive (2002/58/EC) of the European Union (EU). This Directive is now set to be superseded by an ePrivacy Regulation, a draft of which was presented by the European Commission at the beginning of 2017. In future, rules for the protection of personal data and privacy will also apply to instant messaging services. One aim of the European Commission is to ensure that a message sent via a smartphone app enjoys the same level of protection as a text message. The Regulation is intended to particularise and complement the European General Data Protection Regulation (GDPR), which comes into force in May 2018.

The Federation of German Consumer Organisations (vzbv) criticises that – despite a number of consumer-friendly provisions – the draft does not contain any restrictions to offline tracking. This practice is used by companies to monitor the movement of consumers in the vicinity of their shops by locating their smartphones.

CONSUMERS DEMAND CONTROL OVER THEIR MOVEMENT DATA

Retailers are already able to identify ① people, and to track their movements ② and the length of their stay, ③ through the Wi-Fi and Bluetooth connections of their smartphones.





Representative survey conducted by forsa on behalf of vzbv. April 2017. n = 1,002 aged 18 or over. © vzbv

VZBV'S POSITION

Regulation of modern communication services: The scope of the ePrivacy Regulation must be extended to cover services such as email, Voice-over-IP (VoIP) and instant messaging.

Protection for users against monitoring of their activities: The information held on smartphones reveals a lot about their users. Processing of this information should therefore only be permitted with the user's consent – for example when companies want to track user behaviour across websites, apps or mobile devices with cookies and similar technologies to create profiles. Essentially, smartphones and web browsers should be pre-set to protect personal data by default.

Protection of communication content: The content of online chats, messages and emails reveals a lot about consumers. The analysis and processing of communication content must always require explicit consent.

Guaranteed high level of data security: Providers should be obliged to protect user data and communication content using the best available technology. The monitoring of internet communication via software or hardware using a backdoor must be prohibited.

FACTS AND FIGURES

Few consumers in Germany trust companies to sufficiently protect their personal data. An EU survey from 2015 showed that only 32 percent of consumers trusted landline or mobile phone companies and internet service providers, and only 19 percent trusted online businesses.[1]

In the same survey, 70 percent of consumers were particularly concerned about their information being used for a different purpose from the one it was collected for – e.g. for profiling or online behavioural advertising.[2]

A survey conducted by the Vodafone Institute for Society and Communications in January 2016 confirms consumers' distrust when it comes to data protection. 56 percent of respondents stated that they do not put personal information into emails or text messages because they are worried about access by third parties.[3] Another 36 percent said that they did not use social media at all in order to protect their data.[4] vzbv therefore thinks that this makes a consumer-friendly ePrivacy Regulation all the more important in order to restore consumer trust.

MONITORED AT EVERY TURN?

Sabrina enjoys shopping for shoes. In a department store, she looks at a pair of boots that she likes very much. But they are too expensive. Sabrina walks away, but then returns, hesitating. Definitely not? No, definitely not! As she is walking through another department, she gets a surprise: on one of the advertising screens she sees exactly the boots that she has just been looking at. Surely a coincidence. But when she visits another branch of the same department store a few days later the same thing happens again. A monitor is showing the same boots. This is starting to get a bit creepy. How can the monitors recognise her, and how do they know what she is interested in?

Sabrina knows that when she is looking for new riding boots on the internet, related adverts will appear on other websites over the next few days, as if by magic. She does a bit of research and discovers that her smartphone sends out a unique identification code – used, for instance, to establish Wi-Fi or Bluetooth connections. Companies can pick up this code and use it to identify consumers. This enables retailers, for example, to identify people who are repeatedly passing by their shop window. The movement of visitors within a shop can be tracked in the same way. Sabrina is annoyed that this sort of thing is being done without her consent.

An unrealistic scenario? Not at all. The company Renew put up rubbish bins in London fitted with advertising screens that were able to recognise pedestrians by their Wi-Fi-enabled devices, with the intention of showing them personalised adverts.[5] The project had to be halted following protests – but in future that sort of practice would face few restrictions.

1 European Commission: Special Eurobarometer 431; 2015; Page 66; http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_en.pdf; 6 March 2017
2 European Commission: Special Eurobarometer 431; 2015; Page 69 http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_en.pdf; 6 March 2017
3 Vodafone Institute for Society and Communication: Big Data – A European Survey on the Opportunities and Risks of Data Analytics; Page 53; 2016 http://www.vodafone-institut.de/wp-content/uploads/2016/01/VodafoneInstitute-Survey-BigData-en.pdf; 6 March 2017
4 Vodafone Institute for Society and Communication: Big Data – A European Survey on the Opportunities and Risks of Data Analytics; Page 76; 2016 http://www.vodafone-institut.de/wp-content/uploads/2016/01/VodafoneInstitute-Survey-BigData-en.pdf; 6 March 2017
5 Ars Technica: No, this isn't a scene from Minority Report. This trash can is stalking you; https://arstechnica.com/security/2013/08/no-this-isnt-a-scene-from-minoritytyreport-this-trash-can-is-stalking-you; 6 March 2017

verbraucherzentrale Bundesverband

Verbraucherzentrale Bundesverband e.V. (vzbv)
Federation of German Consumer Organisations
Rudi-Dutschke-Straße 17, 10969 Berlin – Germany
Phone +49 30 258 00-0
digitales@vzbv.de

Responsible for the content:
Klaus Müller, vzbv Executive Director
Copy and Design: construktiv GmbH
Infographic, p. 1: vzbv/dpa infografik,
Picture, p. 2: Blackzheep/shutterstock.com