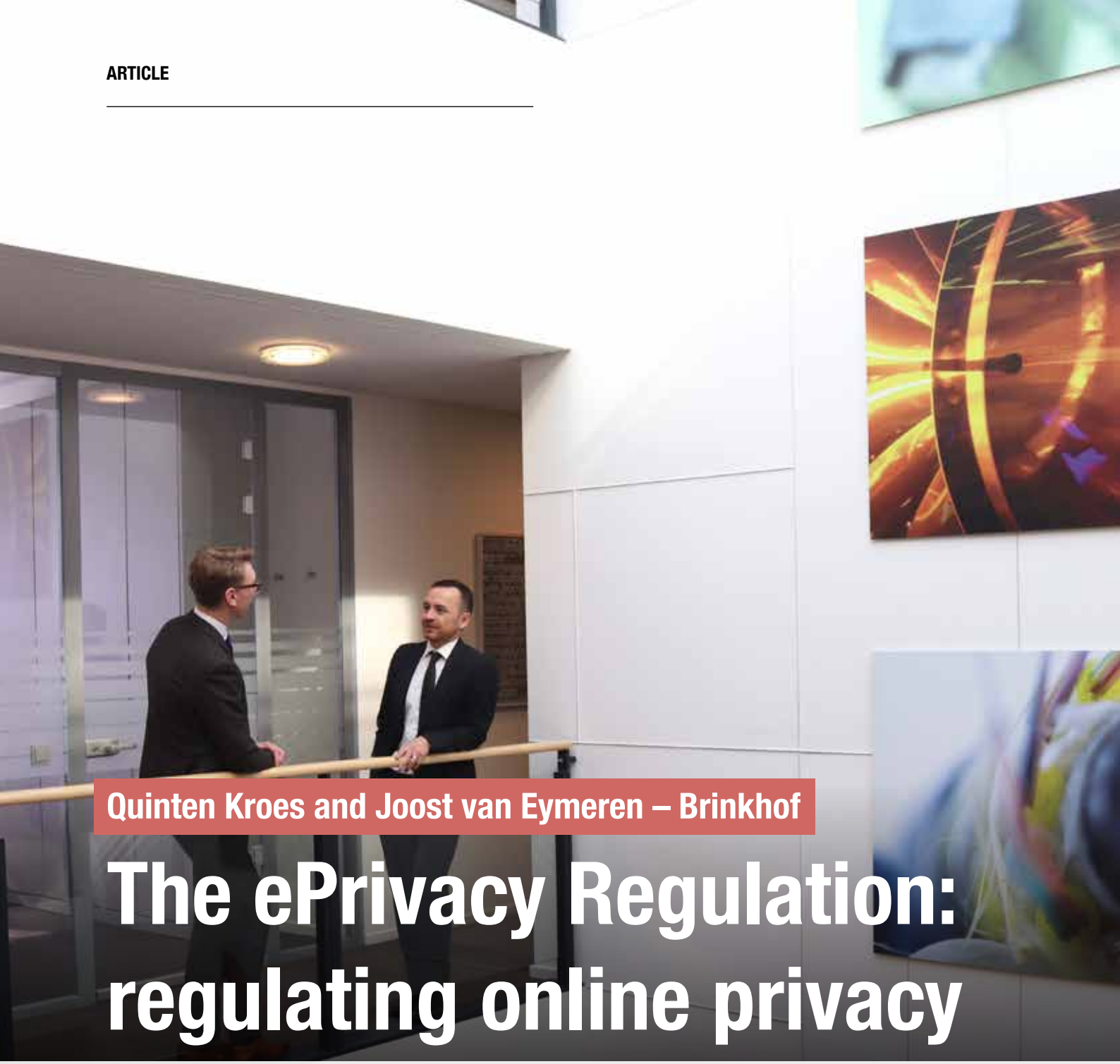

Quinten Kroes and Joost van Eymeren – Brinkhof

The ePrivacy Regulation: regulating online privacy

It has been approximately a year since the GDPR entered into force. And although many organisations are still struggling to meet new requirements such as those around data portability and mandatory data protection officers, additional privacy rules are being debated in Brussels. This next big piece of EU privacy legislation is meant to replace existing data protection rules for the electronic communications sector. However, its scope is not limited to providers of traditional telecommunications services. It will also apply to providers of 'over-the-top' services who offer similar services (for example Skype and WhatsApp).

Moreover, it will regulate important technologies like cookies, data processing by apps and wifi-tracking. Originally this so-called ePrivacy Regulation was meant to enter into force at the same time as the GDPR. However, this has proven too ambitious. The European Commission presented its proposal for the new regulation in January 2017, and its text is currently still under consideration by the Council, which means there is still some way to go before it will be adopted, with the upcoming European elections likely to cause further delay. But bearing in mind that it took some six years for the GDPR to be adopted, this should not come as a surprise.

GDPR vs. ePrivacy

Whereas the GDPR protects privacy by regulating the processing of personal data, the ePrivacy Regulation aims to protect the secrecy of communications. However, given the enhanced and robust data protection framework that the GDPR already provides, it is a valid question what the ePrivacy Regulation can meaningfully add. In 2018, the Centre for Information Policy Leadership (CIPL) in Brussels published a study we conducted into this specific question.

In doing so, we looked at some of the provisions of the Commission's proposal which are likely to have the biggest impact: the rules on the confidentiality of electronic communications data, and those dealing with the protection of information stored in or emitted by end-users' equipment.

- The scope of the ePrivacy Regulation will be broader than the current ePrivacy Directive and will also apply to over-the-top (OTT) providers of communication services (like Skype and WhatsApp), and introduce rules on the collection of information emitted by terminal equipment (for example: wifi tracking).
- The ePrivacy Regulation's heavy reliance on 'consent' as legal basis for data processing may hinder technological innovation.
- The text of the ePrivacy Regulation has not been agreed between the European Parliament and the Council which means that it will probably take at least until the second half of 2019 before there is a final text.

The general principle is that metadata and content must be kept confidential. There are only limited exceptions to this rule, and in many instances this requires the consent of the end-user. For end-user equipment (which could be anything from a mobile phone, a TV settop box, a smart thermostat or a connected car), the principle is the same. The use of processing and storage capabilities of end-users' equipment by any party other than the end-user is prohibited, and so is the collection of information emitted by such equipment, unless that party can rely on an exception (like the consent of the end-user).

This is quite different from the general principles of the GDPR, which allow processing of personal data if the controller is able to rely on one of six alternative legal grounds. Consent is one of these grounds, but in many instances a service provider may also be entitled to process data because this is necessary to perform the contract with the data subject, or because of a legitimate interest of the data controller or a third party, which outweighs the privacy interests of the data subject. This open-ended, principle based system allows a tailored approach which takes account of the risks and other circumstances of a particular situation. The ePrivacy's heavy reliance on 'consent' as the only legal basis for data processing eliminates this flexibility. While no one will call into question the importance of online privacy, it is not obvious that this more rigid approach is always an improvement.

This can be illustrated with some specific use case, which we also addressed in our study for CIPL.

Use cases: fraud prevention and machine learning

A large online trading platform, which allows non-professional traders to sell products to consumers, applies a variety of fraud prevention tools to protect both its traders and their new customers. One technology it wants to implement is a form of device fingerprinting. It will obtain information like the type of device (hardware/OS version), language settings used, IP-address and connection type (e.g. use of proxy-servers), for both traders and buyers, and use this as a factor to determine a risk profile. If the overall risk profile of a trader or buyer exceeds a certain level, the trading platform may act on this information to protect its own interests and those of the users of its platform, by sending a warning, preventing a transaction and/or blocking a user.

Under the ePrivacy Regulation, this particular form of device fingerprinting will have to be based on prior consent of the end-user. However, consent of the end-user is problematic in the context of fraud prevention, as end-users with fraudulent intent are unlikely to provide it.

If this were assessed under the existing framework of the GDPR, the processing of online identifiers provided by the device of a user is likely to qualify as processing of personal data, especially if this is collected together with additional information like an IP-address, and is used for (risk) profiling purposes. As a consequence, this processing will have to comply with the GDPR. It is likely that this particular use of device fingerprinting may be based

on the platform (or its users') legitimate interests, which outweigh the privacy interests of the data subjects, provided that suitable safeguards will have been implemented.

Another problematic use case is the processing of customer support conversations to develop an AI support agent using a big data approach. Again, under the ePrivacy Regulation collection and analysis of data would require consent, whereas under the GDPR a case could be made for processing to be based on the legitimate interest.

Conclusion

The use cases illustrate that ePrivacy Regulation's more rigid approach may have unintended outcomes and not always be preferable to the risk-based approach allowed under the GDPR.

In other instances, the ePrivacy Regulation merely duplicates what is already in the GDPR, and does not actually add anything much to the existing body of law. For example, while the ePrivacy Regulation imposes a general obligation to erase communications data when it is no longer necessary for the provision of the service, a similar duty will already apply under the GDPR's storage limitation and data minimisation requirements. Also from this perspective, it is not always obvious to see the added value of this new law.

"The ePrivacy's heavy reliance on 'consent' as the only legal basis for data processing eliminates flexibility."

The process of adopting the new rules has turned out to be more drawn out than originally expected, giving rise to repeated calls from regulators for more expediency in the legislative process. However, given the complex interplay between the general framework of the GDPR and the specific ePrivacy rules, and the very real risk of unintended regulatory consequences for the fast moving world of online privacy, this is hardly surprising. Rushing this important process might end up being a case of acting in haste, and repenting at leisure.

About the author
Quinten Kroes is partner privacy and data protection at Brinkhof. Quinten has been active as a lawyer in the telecommunications, media and technology sectors since 1995, advising and litigating about matters of telecommunications, media and data protection law.

About the author
Joost van Eymeren is a lawyer at Brinkhof. Joost specialises in technology and data protection law, advising clients on privacy compliance and drafting and negotiating commercial contracts, including IT and licensing agreements.