EU

EU Council Adopts the Network and Information Security Directive

On 17 May 2016, the EU Council adopted its position at first reading of the Network and Information Security Directive (NIS Directive). First proposed by the European Commission in 2013, the Directive has been designed to bolster cooperation between the Member States on cybersecurity issues. The NIS requires each Member State to formulate a strategy to deal with cyber threats, and assign responsibility to one or more competent authority to handle the security of network and information systems issues. It will impose security obligations on "operators of essential services" in critical sectors such as energy, transport, banking, health and water supply, and on "digital service providers". These providers will be obliged to take active steps to manage cyber risks and report major security breaches to the relevant competent authority. The NIS Directive now needs to be approved by the European Parliament. It is expected to enter into force in August 2016, but thereafter Member States will have 21 months to adopt the necessary national provisions and then 6 months to identify operators of essential services.

Press release

The Court of Justice of the EU Advises that IP Addresses are Personal Data

The Advocate General of the Court of Justice of the EU has handed down a non-binding opinion in *Patrick Breyer v. Federal Republic of Germany,* declaring that IP addresses are personal data and as such should be protected by data protection laws. Specifically, he stated this would be the case where internet service providers held additional information that when combined with an IP address could reveal the identity of the user. While this opinion is not binding, it is highly persuasive and the Court is expected to hand down its final decision shortly.

The opinion (in German)

France

The CNIL Publishes Blanket Authorisations for Data Controllers in the Healthcare Sector

On 14 April 2016, the Commission Nationale de l'Informatique et des Libertés (CNIL) published three blanket authorisations for data controllers that operate in the social and healthcare sector. A blanket authorisation ("authorisation unique") allows for a simplified registration procedure, where the data controller self certifies that its processing conforms to a "norm" dictated by the CNIL. The three blanket authorisations are AU 074 (social and medical assistance and monitoring of disabled and elderly persons); AU 048 (social assistance and monitoring of person in difficulties); and AU 049 (social assistance and monitoring within prevention and protection of minors and young adults)**.** They are intended to be the first part of a "compliance pack" to be implemented by the CNIL in this sector.

Press release (in French)

Germany

Bundesrat Debates Criminal Prosecution of "Gawkers "

The Federal States of Niedersachsen, Berlin and Mecklenburg-Vorpommern have submitted an initiative to the Bundesrat that would criminalise individuals who "gawk" at accidents by taking photographs or making video recordings. One of the main goals of the initiative is to better protect the privacy rights of the deceased. Accordingly, under these new rules anyone disturbing the emergency services by "gawking" at an accident can be penalised with imprisonment for up to one year or with a fine.

Press release (in German)

US

U.S. Supreme Court Issues Opinion in Spokeo, Inc. v. Robins

On May 16, 2016, the U.S. Supreme Court issued its opinion in *Spokeo, Inc. v. Robins.* It held that a plaintiff must allege "concrete" and particular harm in order to have standing to bring a suit in the US federal court. The Court ruled that the fact that a statute may provide for statutory damages for violations is not, by itself, sufficient to confer standing on a plaintiff. While this case arose under the US Fair Credit Reporting Act, it will be relevant to class actions asserting violations of privacy laws and other consumer protection laws, including the Telephone Consumer Protection Act ("TCPA"). Many of these laws provide for statutory damages for violations, but do not specify that a plaintiff must have suffered actual harm as a result of the violation. Following this decision, plaintiffs will be required to allege and then demonstrate that they suffered specific harm as a result of the violation of the law; it will no longer be enough to merely assert that the law itself was violated.

The opinion

US Senate Committee on Commerce, Science, & Transportation Holds Hearing Entitled "The Telephone Consumer Protection Act at 25: Effects on Consumers and Business

The Senate Committee has heard from consumer advocacy groups, industry representatives, and independent experts in relation to the effects of the TCPA. Monica Desai, a Communications Practice partner in our Washington DC office and a former Federal Communications Commission official, testified as an expert about how consumers have used the TCPA to bring abusive lawsuits against companies for technical violations of the TCPA which did not result in any actual harm. Ms. Desai pointed out that even companies with robust compliance programs have been sued for technical violations of the TCPA and have had to pay steep attorney's fees that are disproportionate to the amount of actual injury suffered.

Click here for more information and the witnesses' testimony.

Contact

Annette Demmel
Partner, Berlin
T +49 30 7261 68 108
E annette.demmel@squirepb.com

Stephanie Faber
Of Counsel, Paris
T +33 1 5383 7583
E stephanie.faber@squirepb.com

Deborah Lodge
Partner
T +1 202 457 6030
E deborah.lodge@squirepb.com

Caroline Egan
Consultant
T +44 121 222 3386
E caroline.egan@squirepb.com

Francesca Fellowes
Senior Associate
T +44 113 284 7459
E franscesca.fellowes@squirepb.com