Brussels, 15 May 2019

Dear Vice-President Andrus Ansip
Dear Commissioner Mariya Gabriel,
Dear Commissioner Vera Jourová,
Dear Chair of the European Data Protection Board Andrea Jelinek,
Dear Chair of the Body of European Regulators for Electronic Communications Jeremy Godfrey,
Dear European Data Protection Supervisor Giovanni Buttarelli,

CC:
Head of Cabinet of Commissioner Gabriel Lora Borissova
Deputy Head of Cabinet of Commissioner Gabriel Carl-Christian Buhr
Wolf-Dietrich Grussmann, DG Connect
Agnieszka Bielinska, DG Connect
Irene Roche-Laguna, DG Connect
Eric Gaudillat, DG Connect
National Regulatory Authorities and Data Protection Authorities of the EEA

We are writing you in the context of the evaluation of Regulation (EU) 2015/2120 and the reform of the BEREC Guidelines on its implementation. Specifically, we are concerned because of the increased use of Deep Packet Inspection (DPI) technology by providers of internet access services (IAS). DPI is a technology that examines data packets that are transmitted in a given network beyond what would be necessary for the provision IAS by looking at specific content from the part of the user-defined payload of the transmission.

IAS providers are increasingly using DPI technology for the purpose of traffic management and the differentiated pricing of specific applications or services (e.g. zero-rating) as part of their product design. DPI allows IAS providers to identify and distinguish traffic in their networks in order to identify traffic of specific applications or services for the purpose such as billing them differently throttling or prioritising them over other traffic.

The undersigned would like to recall the concerning practice of examining domain names or the addresses (URLs) of visited websites and other internet resources. The evaluation of these types of data can reveal sensitive information about a user, such as preferred news publications, interest in specific health conditions, sexual preferences, or religious beliefs. URLs directly identify specific resources on the world wide web (e.g. a specific image, a specific article in an encyclopedia, a specific segment of a video stream, etc.) and give direct information on the content of a transmission.

A mapping of differential pricing products in the EEA conducted in 2018 identified 186 such products which potentially make use of DPI technology.[1] Among those, several of these products by mobile operators with large market shares are confirmed to rely on DPI because their products offer providers of applications or services the option of identifying their traffic via criteria such as Domain names, SNI, URLs or DNS snooping.[2]

Currently, the BEREC Guidelines[3] clearly state that traffic management based on the monitoring of domain names and URLs (as implied by the phrase "transport protocol layer payload") is not "reasonable traffic management" under the Regulation. However, this clear rule has been mostly ignored by IAS providers in their treatment of traffic.

The nature of DPI necessitates telecom expertise as well as expertise in data protection issues. Yet, we observe a lack of cooperation between national regulatory authorities for electronic communications and regulatory authorities for data protection on this issue, both in the decisions put forward on these products as well as cooperation on joint opinions on the question in general. For example, some regulators issue justifications of DPI based on the consent of the customer of the IAS provider which crucially ignores the clear ban of DPI in the BEREC Guidelines and the processing of the data of the other party communicating with the subscriber, which never gave consent.

Given the scale and sensitivity of the issue, we urge the Commission and BEREC to carefully consider the use of DPI technologies and their data protection impact in the ongoing reform of the net neutrality Regulation and the Guidelines. In addition, we recommend to the Commission and BEREC to explore an interpretation of the proportionality requirement included in Article 3, paragraph 3 of Regulation 2015/2120 in line with the data minimization principle established by the GDPR. Finally, we suggest to mandate the European Data Protection Board to produce guidelines on the use of DPI by IAS providers.

Best regards,

Academics and Individuals:

Kai Rannenberg, Chair of Mobile Business & Multilateral Security, Goethe University Frankfurt, Germany
Stefan Katzenbeisser, Chair of Computer Engineering, University of Passau, Germany
Max Schrems, Privacy Activist, Austria
Klaus-Peter Löhr, Professor für Informatik (a.D.), Freie Universität Berlin, Germany
Joachim Posegga, Chair of IT-Security, University of Passau, Germany
Dominik Herrmann, Chair for Privacy and Security in Information Systems, University of Bamberg, Germany
Rigo Wenning, AFS Rechtsanwälte, ERCIM Legal Counsel, Vorstand EDV-Gerichtstag, Fitug e.V., France

1 See https://epicenter.works/document/1522 page 19-21, 34-35 and 38-40.
2 Cf.
3 BoR (16) 127, paragraphs 69 and 70.

Douwe Korff, Emeritus Professor of International Law, London Metropolitan University, United Kingdom
Dr. TJ McIntyre, UCD Sutherland School of Law, United Kingdom
Dr Ian Brown, Senior Fellow, Research ICT Africa / CyberBRICS visiting professor, Fundação Getúlio Vargas Direito Rio, Brazil
Dr. Jef Ausloos (Institute for Information Law (IViR) - University of Amsterdam), Netherlands
Paddy Leersen LL.M., PhD Candidate University of Amsterdam, Non-Residential Fellow Stanford University Center for Internet & Society, Netherlands
Simone Fischer Hübner, Professor in Computer Science, Karlstad University, Sweden
Erich Schweighofer, Head of the Centre for Computers and Law, Department of European, International and Comparative Law, University of Vienna, Austria
Prof. Dr.-Ing. Christoph Sorge, Saarland University, Germany
Frederik J. Zuiderveen Borgesius, Professor of Law at iCIS Institute for Computing and Information Sciences, Radboud University

NGOs and NPOs:

European Digital Rights, Europe
Electronic Frontier Foundation, International
Council of European Professional Informatics Societies, Europe
Article 19, International
Chaos Computer Club e.V, Germany
epicenter.works - for digital rights, Austria
Austrian Computer Society (OCG), Austria
Bits of Freedom, the Netherlands
La Quadrature du Net, France
ApTI, Romania
Code4Romania, Romania
IT-Pol, Denmark
Homo Digitalis, Greece
Hermes Center, Italy
X-net, Spain
Vrijschrift, the Netherlands
Dataskydd.net, Sweden
Electronic Frontier Norway (EFN), Norway
Alternatif Bilisim (Alternative Informatics Association), Turkey
Digitalcourage, Germany
Fitug e.V., Germany
Digitale Freiheit, Germany
Deutsche Vereinigung für Datenschutz e.V. (DVD), Germany
Gesellschaft für Informatik e.V. (GI), Germany
LOAD e.V. - Verein für liberale Netzpolitik, Germany
Swiss Informatics Society (SI), Switzerland
German Chapter of the ACM e.V.

Companies:

Wire Swiss GmbH, Switzerland, Alan Duric, CTO/COO & Co-Founder
Research Institute - Digital Human Rights Center, Austria
Fédération des Fournisseurs d'Accès Internet Associatifs, France
Baycloud Systems, United Kingdom, Mike O'Neill, Director