



TEXTS ADOPTED

P8_TA(2018)0433

The use of Facebook users' data by Cambridge Analytica and the impact on data protection

European Parliament resolution of 25 October 2018 on the use of Facebook users' data by Cambridge Analytica and the impact on data protection (2018/2855(RSP))

The European Parliament,

- having regard to the Treaty on European Union (TEU), the Treaty on the Functioning of the European Union (TFEU), the Charter of Fundamental Rights of the European Union, notably its Articles 7, 8, 11, 12, 39, 40, 47 and 52, the Convention for the Protection of Human Rights and Fundamental Freedoms, notably its Articles 8, 9, 10, 11, 13, 16 and 17, and the Protocol to the Convention for the Protection of Human Rights and Fundamental Freedoms, notably its Article 3,
- having regard to the International Covenant on Civil and Political Rights, notably its Articles 2, 17, 19, 20 and 25,
- having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)¹, and to Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA²,
- having regard to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and its Additional Protocol,
- having regard to the House of Commons inquiry into fake news and its Digital, Culture, Media and Sport Committee's 5th Interim Report on Disinformation and 'fake news',
- having regard to the hearings held in the US House of Representatives Committee on Energy and Commerce,

¹ OJ L 119, 4.5.2016, p. 1.

² OJ L 119, 4.5.2016, p. 89.

- having regard to Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield¹,
- having regard to its resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield²,
- having regard to the judgment of the Court of Justice of the European Union (CJEU) of 6 October 2015 in Case C-362/14 *Maximillian Schrems v Data Protection Commissioner*³,
- having regard to the judgment of the CJEU of 25 January 2018 in Case C-498/16 *Maximilian Schrems v Facebook Ireland Limited*⁴,
- having regard to the judgment of the CJEU of 5 June 2018 in Case C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*⁵,
- having regard to the filing of the formal request by David Caroll requesting that Cambridge Analytica recover his personal information and reveal its source,
- having regard to Opinion 3/2018 of the European Data Protection Supervisor (EDPS) of 19 March 2018 on online manipulation and personal data⁶,
- having regard to the Guidelines of the Article 29 Working Party of 3 October 2017 on Automated individual decision-making and Profiling for the purposes of Regulation (EU) 2016/679⁷,
- having regard to the two sets of written replies to the questions that were left unanswered at the meeting between European Parliament political group leaders and Facebook CEO Zuckerberg, published by Facebook on 23 May⁸ and 4 June 2018 respectively⁹,
- having regard to Commission Recommendation (EU) 2018/234 of 14 February 2018 on enhancing the European nature and efficient conduct of the 2019 elections to the European Parliament¹⁰, Commission Recommendation of 12 September 2018 on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns in the context of elections to the European Parliament (C(2018)5949), and the Commission communication of 12

¹ OJ L 207, 1.8.2016, p. 1.

² Texts adopted, P8_TA(2018)0315.

³ ECLI:EU:C:2015:650.

⁴ ECLI:EU:C:2018:37.

⁵ ECLI:EU:C:2018:388.

⁶ https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf

⁷ http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

⁸ <http://www.europarl.europa.eu/the-president/en/newsroom/answers-from-facebook-to-questions-asked-during-mark-zuckerberg-meeting>

⁹ <http://www.europarl.europa.eu/resources/library/media/20180604RES04911/20180604RES04911.pdf>

¹⁰ OJ L 45, 17.2.2018, p. 40.

- September 2018 entitled ‘Securing free and fair European elections’ (COM(2018)0637),
- having regard to the Commission proposal of 12 September 2018 for a regulation of the European Parliament and of the Council amending Regulation (EU, Euratom) No 1141/2014 as regards a verification procedure related to infringements of rules on the protection of personal data in the context of elections to the European Parliament (COM(2018)0636),
 - having regard to the Commission guidance of 12 September 2018 on the application of Union data protection law in the electoral context (COM(2018)0638),
 - having regard to the in-depth hearings conducted by the Committee on Civil Liberties, Justice and Home Affairs, mandated by the European Parliament, on the use of Facebook users’ data by Cambridge Analytica and the impact on data protection,
 - having regard to the reports of the Information Commissioner’s Office of the United Kingdom on the investigation into the use of data analytics in political campaigns, and the report entitled ‘Democracy disrupted’¹,
 - having regard to the testimonial by the European Consumer Organisation (BEUC) presented on 25 June 2018²,
 - having regard to the statement by the Commission of 23 October 2018,
 - having regard to the motion for a resolution of the Committee on Civil Liberties, Justice and Home Affairs,
 - having regard to Rule 123(2) of its Rules of Procedure,
- A. whereas investigative journalism uncovered and made public major data leaks of Facebook user data in relation to the access that was granted by Facebook to third-party applications, and the subsequent abuse of this data for the purposes of electoral campaigning efforts as well as other breaches of personal data held and gathered by major social media companies that came to light afterwards;
- B. whereas these personal data breaches had an impact on citizens across the globe, including European and non-European citizens residing on European Union territory; whereas various national parliaments conducted hearings, inquiries and published findings on the matter;
- C. whereas these personal data breaches occurred over an extended period of time; whereas the companies concerned were in breach of EU data protection law applicable at that time, in particular Directive 95/46/EC and Directive 2002/58/EC;
- D. whereas the data misuse which was revealed in the context of the Cambridge Analytica

¹ <https://ico.org.uk/media/action-weve-taken/2259369/democracy-disrupted-110718.pdf>
<https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/07/findings-recommendations-and-actions-from-ico-investigation-into-data-analytics-in-political-campaigns/>

² http://www.beuc.eu/publications/beuc-x-2018-067_ep_hearing_facebook-cambridge_analytica.pdf

scandal happened before the application of the General Data Protection Regulation (GDPR);

- E. whereas Facebook has affirmed that no bank account, credit card or national identity information was shared with Cambridge Analytica;
- F. whereas Cambridge Analytica claimed the data processing was officially carried out for research purposes, but subsequently passed on the data gathered for political and commercial use;
- G. whereas the initial reaction by the companies concerned did not meet the expected standards and did not enable a full and independent investigation and audit by the authorities concerned either at national or European level;
- H. whereas the chairs of the political groups in the European Parliament held a first exchange of views in camera with the CEO and founder of Facebook, Mark Zuckerberg, on 22 May 2018, and this meeting resulted in the request by the Conference of Presidents for the Committee on Civil Liberties, Justice and Home Affairs, in association with the Committees on Constitutional Affairs, Legal Affairs and Industry, Research and Energy, to hold in-depth follow-up hearings;
- I. whereas three hearings on the impact of the Facebook/Cambridge Analytica case on issues related to data protection, electoral processes, fake news and the market position of social media were held on 4 and 25 June and 2 July 2018 with the participation of the European Commissioners concerned, the Executive Director of the European Union Agency for Network and Information Security (ENISA), the EDPS, the Chair of the European Data Protection Board (EDPB), the UK Information Commissioner's Office, the Chief Executive of the UK Electoral Commission, citizens concerned and Facebook;
- J. whereas Facebook refused to delegate staff members with the appropriate level of responsibility and in possession of the necessary technical expertise and knowledge requested by the Committee Chairs concerned, sending public policy team members to all three hearings instead; whereas the information provided by the Facebook representatives during the hearings lacked precision on the concrete and specific measures taken to ensure full compliance with EU data protection law and was of a more general nature;
- K. whereas in Opinion 3/2018, the EDPS expresses several concerns on the issues of online manipulation and personal data; whereas the EDPS also argues that competition law has a crucial role in ensuring the accountability of dominant players in the market and protecting democracy against excessive market power; whereas the interests of individuals should be better reflected in assessing the potential abuse of dominance or the mergers of companies, which may have accumulated significant informational power;
- L. whereas in its Opinion of 3 October 2017, the Article 29 Working Party stated that profiling and automated decision-making can pose significant risks for individuals' rights and freedoms which require appropriate safeguards;
- M. whereas the Chair of the EDPB highlighted that the Facebook/Cambridge Analytica case occurred before the entry into force of the GDPR, and therefore the system of Lead

Supervisory Authority under the GDPR does not apply; whereas the investigations were led by the UK Information Commissioner's Office;

- N. whereas Facebook has admitted that it entered into a contract with an application developer without having conducted a prior check of its terms and conditions, which reserved the right for the latter to disclose personal data to third parties; whereas this oversight had grave consequences and such a practice was already illegal under the then applicable data protection law;
- O. whereas negotiations are currently ongoing on the e-Privacy Regulation;
- P. whereas the EDPB indicated that around 100 cross-border cases are already being dealt with in the framework of the consistency mechanism under the GDPR; whereas this mechanism coordinates the actions of national data protection authorities in order to ensure a common approach to the enforcement of EU data protection law;
- Q. whereas Facebook, a signatory to the Privacy Shield, has confirmed that the personal data of up to 2.7 million EU citizens were among those improperly used by political consultancy Cambridge Analytica;
- R. whereas on 28 September 2018, Facebook made public that an external actor had attacked its systems and exploited a vulnerability that exposed Facebook access tokens for 50 million accounts, and whereas the Irish Data Protection Commission and other data protection authorities have started investigations into these facts in order to assess compliance with EU data protection law;
- S. whereas the US Federal Trade Commission is currently investigating whether Facebook failed to honour its privacy promises, including compliance with the Privacy Shield, or whether it engaged in unfair acts that caused substantial injury to consumers in violation of the Federal Trade Commission (FTC) Act and the previous settlement between the FTC and Facebook reached in 2011;
- T. whereas four consumer organisations of Belgium, Italy, Spain and Portugal have launched a collective redress action against Facebook, claiming economic compensation for affected Facebook users in their respective countries;
- U. whereas the BEUC stated in its testimonial presented on 25 June 2018 that it is necessary to ensure platform accountability for third-party access to personal data; whereas the BEUC also argues in the same testimonial that companies should do more to ensure solid accountability structures for partner access to personal data and the further exploitation of this data;
- V. whereas the investigation by the Information Commissioner's Office of the United Kingdom also covered the link between Cambridge Analytica, its parent company SCL Elections Limited and Aggregate IQ, and involves allegations that personal data, obtained from Facebook, may have been misused by both sides in the UK referendum on membership of the EU and used to target voters during the 2016 American presidential election process; whereas the investigation by the Information Commissioner's Office of the United Kingdom was mainly conducted under the Data Protection Act 1998 and under the Privacy and Electronic Communications Regulations (PECR) 2003, while also extrapolating ahead to the GDPR where appropriate;

- W. whereas the UK House of Commons Culture, Media and Sport Select Committee heard evidence that showed alleged Russian interference in electoral processes in the EU, and urged the responsible national authorities to investigate these allegations; whereas in the US, a Special Counsel was appointed in May 2017 to investigate Russian interference in the 2016 presidential elections and related matters, and whereas this investigation is ongoing;
- X. whereas the Information Commissioner's Office of the United Kingdom has issued Facebook with a Notice of Intent to issue a monetary penalty in the sum of GBP 500 000 for lack of transparency and security issues relating to the harvesting of data constituting breaches of the first and seventh data protection principles under the Data Protection Act 1998;
- Y. whereas the Information Commissioner's Office of the United Kingdom has already issued 23 Information Notices to 17 different organisations and individuals, including Facebook, on 23 February 2018, to request provision of information from the organisations in a structured way; whereas Facebook confirmed on 18 May 2018 that Aggregate IQ had created and, in some cases, placed advertisements on behalf of the Democratic Unionist Party's (DUP) Vote to Leave campaign, Vote Leave, BeLeave and Veterans for Britain;
- Z. whereas the Information Commissioner's Office of the United Kingdom has expressed its concerns as regards the terms of the information available to users about the sources of the data and the availability and transparency of the controls offered to users; whereas the Information Commissioner's Office of the United Kingdom also stated that the overall privacy information and controls made available by Facebook did not effectively inform the users about the likely uses of their personal information; whereas the Information Commissioner's Office of the United Kingdom has raised concerns about cases in which data was accessed from the Facebook platform and used for purposes it was not intended for, or that data subjects would not reasonably have expected;
- AA. whereas figures from the Electoral Commission of the UK have shown that the political parties in the United Kingdom spent GBP 3,2 million on direct Facebook advertising during the 2017 general election;
- AB. whereas social networks constitute an important platform for political parties and public institutions by allowing them to connect with citizens;
- AC. whereas global online platforms face challenges in countering false news effectively, given the differing threats and media landscapes in different countries and regions;
- AD. whereas data analysis and algorithms have an increasing impact on the information made accessible to citizens; whereas such techniques, if misused, may endanger fundamental rights to information as well as media freedom and pluralism;
- AE. whereas algorithmic accountability and transparency is essential to ensure that individuals have proper information about and a clear understanding of the processing of their personal data; whereas it should mean implementing technical and operational measures that ensure transparency, and non-discrimination through automated decision-making, and that ban the calculating of probabilities of individual behaviour; whereas

transparency should give individuals meaningful information about the logic involved, the significance and the envisaged consequences; whereas this should include information about the data used for training big data analytics and allow individuals to understand and monitor the decisions affecting them;

- AF. whereas at the meeting with European Commissioners on 2 July 2018, Facebook promised to cooperate and give access to the data about the alleged voting manipulation to independent academics;
1. Expects all online platforms to ensure full compliance with EU data protection law, namely the GDPR and Directive 2002/58/EC (e-Privacy), and to help users understand how their personal information is processed in the targeted advertising model, and that effective controls are available, which includes ensuring that separate consents are used for different purposes of processing, and that greater transparency is in place in relation to the privacy settings, and to the design and prominence of privacy notices;
 2. Stresses that the research argument exemption in EU data protection law can never be used as a loophole for data misuse;
 3. Takes note of Facebook's statement that it exclusively uses the data of non-Facebook users to create aggregated datasets from which it derives conclusions about how the service is used;
 4. Emphasises the need for much greater algorithmic accountability and transparency with regard to data processing and analytics by the private and public sectors and any other actors using data analytics, as an essential tool to guarantee that individuals are appropriately informed about the processing of their personal data;
 5. Takes the view that the digital age requires electoral laws to be adapted to this new digital reality, and suggests that conventional ('offline') electoral safeguards, such as rules applicable to political communications during election periods, transparency of and limits to electoral spending, respect for election silence periods and equal treatment of candidates should also apply online; is of the opinion that Member States should introduce an obligatory system of digital imprints for electronic campaigning and advertising and implement the Commission's Recommendation aimed at enhancing the transparency of paid online political advertisements and communications; stresses that any form of political advertising should include easily accessible and understandable information on the publishing organisation and who is legally responsible for spending so that it is clear who sponsored campaigns, similar to existing requirements for printed campaign materials currently in place in various Member States; insists that citizens of the Union should be able to easily recognise online paid political advertisements and communications, and the party, foundation or organisation behind them; insists, furthermore, that transparency should also include complete information about the criteria for selecting the target group of the specific political advertising and the expected size of the target group;
 6. Notes that Facebook has updated its privacy settings to allow users to opt out from targeting, including the showing of advertisements based on information obtained from third parties, and the use of their personal information collected by Facebook to show advertisements on other websites or platforms;

7. Recommends that all online platforms distinguish political uses of their online advertising products from their commercial uses; recalls that processing personal data for political advertising requires a separate legal basis from the one for commercial advertising;
8. Believes that the requirement to verify the identity, location and sponsor of political advertisements recently introduced by Facebook in the US is a good initiative which will increase transparency and contribute to the fight against election meddling by foreign actors; urges Facebook to introduce the same requirements for political advertisements in Europe; calls on the Member States to adjust their electoral laws to this effect;
9. Believes that profiling for political and electoral purposes and profiling based on online behaviour that may reveal political preferences, such as interaction with political content, in so far as, pursuant to EU data protection law, it refers to political or philosophical opinions, should be prohibited, and is of the opinion that social media platforms should monitor and actively inform the authorities if such behaviour occurs; also believes that profiling based on other data, such as socio-economic or demographic factors, for political and electoral purposes, should be prohibited; calls on political parties and other actors involved in elections to refrain from using profiling for political and electoral purposes; calls on political parties to be transparent as to their use of online platforms and data;
10. Recalls the measures proposed by the Commission for securing free and fair European elections, in particular the legislative amendment to tighten up the rules on European political party funding, creating the possibility to impose financial sanctions for breaching data protection rules in order to deliberately influence the outcome of the European elections; recalls that the processing of personal data by political parties in the EU is subject to the GDPR, and that the breach of the principles, rights and obligations encompassed within this law would result in additional fines and sanctions;
11. Considers election interference to be a huge risk for democracy, the tackling of which requires a joint effort involving service providers, regulators and political actors and parties;
12. Welcomes the package presented by the Commission on 12 September 2018 regarding preparations for the European elections;
13. Recalls Facebook's promise on the issue of giving access to the data about alleged voting manipulation to independent academics, and expects to be informed before the end of 2018 on the main findings and proposed remedies;
14. Notes the actions undertaken by Facebook to counter data misuse, including the disabling or ban of applications suspected of misusing user data; expects Facebook to act swiftly on reports regarding suspicious or abusive applications, and to prevent such applications from being allowed on the platform in the first place;
15. Stresses that social media platforms are not only passive platforms that simply group user-generated content, but highlights that technological developments have widened the scope and role of such companies by introducing algorithm-based advertising and content publication; concludes that this new role should be reflected in the regulatory

field;

16. Notes with regret that Facebook was not willing to send staff members with the appropriate technical qualifications and level of corporate responsibility to the hearings, and points out that such an approach is detrimental to the trust European citizens have in social platforms; regrets that Mark Zuckerberg did not wish to attend a public hearing with Members;
17. Finds that Facebook not only breached the trust of EU citizens, but also EU law, and recalls that during the hearings, a Facebook representative confirmed that Facebook was aware that the terms and conditions of the ‘This is your digital life’ application stated that the data the application collected could be sent to third parties; concludes that Facebook knowingly entered into a contract with an application developer that openly announced that they reserved the right to disclose personal data to third parties; concludes, furthermore, that Facebook is the controller of the personal data and is therefore legally responsible when entering into a contract with a processor that breaches EU data protection law;
18. Takes note of the privacy improvements that Facebook has undertaken after the Facebook/Cambridge Analytica scandal, but recalls that Facebook promised to hold a full internal audit of which the European Parliament has not yet been informed, and recommends that Facebook make substantial modifications to its platform to ensure its compliance with EU data protection law;
19. Urges Facebook to allow and enable ENISA and the EDPB, within the limits of their respective mandates, to carry out a full and independent audit of its platform and to present the findings of this audit to the Commission, the European Parliament and national parliaments; believes that such an audit should also be carried out on other major platforms;
20. Highlights the urgency of countering any attempt to manipulate EU elections and of reinforcing rules applicable to online platforms regarding the disruption of advertising revenues of accounts and websites that spread disinformation; Welcomes the individual roadmaps setting out concrete actions to fight disinformation in all EU Member States which online platforms and the advertising industry presented to the Commission on 16 October 2018; urges online platforms to label content shared by bots by applying transparent rules, to speed up the removal of fake accounts, to comply with court orders to provide details of those creating illegal content, and to work with independent fact-checkers and academia to inform users about disinformation with significant reach and to offer corrections whenever available;
21. Calls on all online platforms providing advertising services to political parties and campaigns to include experts within the sales support team who can provide political parties and campaigns with specific advice on transparency and accountability in relation to how to prevent personal data being used to target users; calls on all online platforms that allow buyers of advertising to make certain selections to provide legal advice on the responsibilities of those buyers as joint controllers of the data, following the judgment of the CJEU in case C-210/16;
22. Calls on all online platforms to urgently roll out planned transparency features in relation to political advertising, which should include consultation and evaluation of

these tools by national authorities in charge of electoral observation and control; insists that such political and electoral advertising should not be done on the basis of individual user profiles;

23. Calls on Member States to adapt the electoral rules on online campaigning, including those pertaining to transparency on funding, election silence periods, the role of the media and disinformation;
24. Recommends that it should be a requirement that third-party audits be carried out after referendum campaigns have been concluded to ensure that personal data held by the campaign is deleted, or, if it has been shared, that the appropriate consent has been obtained;
25. Calls on Facebook to improve its transparency to enable users to understand how and why a political party or campaign might target them;
26. Takes the view that data protection authorities should be provided with adequate funding to build up the same technical expert knowledge as possessed by those organisations under their scrutiny; calls on the Member States to ensure that the data protection authorities are provided with the human, technical and financial resources necessary for the effective performance of their tasks and exercise of their powers, as required under Article 52 of the GDPR; urges the Commission to scrutinise the Member States closely on their obligation to make these resources available, and if necessary, to start infringement procedures;
27. Recalls that Facebook is a self-certified organisation under the EU-US Privacy Shield and, as such, benefited from the adequacy decision as a legal ground for the transfer and further processing of personal data from the European Union to the United States;
28. Recalls its resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield and, in view of the acknowledgement by Facebook that major privacy breaches occurred, calls on the US authorities responsible for enforcing the Privacy Shield to act upon such revelations without delay, in full compliance with the assurances and commitments given to uphold the current Privacy Shield arrangement and, if needed, to remove such companies from the Privacy Shield list; welcomes, in this context, the removal of Cambridge Analytica from the Privacy Shield in June 2018; calls also on the competent EU data protection authorities to investigate such revelations and, if appropriate, suspend or prohibit data transfers under the Privacy Shield; expects the FTC, as the responsible US authority, to provide the Commission with a detailed summary of its findings once it has concluded its investigation into the data breach involving Facebook and Cambridge Analytica, and to take appropriate enforcement action against the companies involved to provide an effective deterrent;
29. Regrets that the deadline of 1 September 2018 for the US to be fully compliant with the Privacy Shield has not been met; considers, therefore, that the Commission has failed to act in accordance with Article 45(5) of the GDPR; urges the Commission therefore, in line with Parliament's resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield, to suspend the Privacy Shield until the US authorities comply with its terms;
30. Notes that the misuse of personal data affects the fundamental rights of billions of

people around the globe; considers that the GDPR and the e-Privacy Directive provide the highest standards of protection; regrets that Facebook decided to move 1.5 billion non-EU users out of the reach of the protection of the GDPR and the e-Privacy Directive; questions the legality of such a move; urges all online platforms to apply the GDPR (and e-Privacy) standards to all of their services, regardless of where they are offered, as a high standard of protection of personal data is increasingly seen as a major competitive advantage;

31. Calls on the Commission to upgrade competition rules to reflect the digital reality and to look into the business model of social media platforms and their possible monopoly situation, taking due account of the fact that such a monopoly could be present as a result of the specificity of the brand and the quantity of personal data that is held rather than it being a traditional monopoly situation, and to take the necessary measures to remedy this; calls on the Commission to propose amendments to the European Electronic Communications Code that also require over-the-top communications providers to interconnect with others, in order to overcome the lock-in effect for their users;
32. Requests that the European Parliament, the Commission, the Council and all other European Union institutions, agencies and bodies verify that the social media pages and the analytical and marketing tools used on their respective websites do not by any means put the personal data of citizens at risk; suggests that they evaluate their current communication policies from that perspective, which may result in them considering closing their Facebook accounts as a necessary condition of protecting the personal data of every individual contacting them; instructs its own communications department to strictly adhere to the EDPS Guidelines on the protection of personal data processed through web services provided by EU institutions¹;
33. Is of the view that the next European Commission should task one of its members specifically with the privacy and data protection portfolio, with a view to proactively engaging partners inside and outside the EU and ensuring that all legislative proposals are fully compliant with the EU legal acquis on privacy and data protection;
34. Urges the Council to end the deadlock on the e-Privacy Regulation, and to finally reach an agreement with Parliament without lowering the level of protection currently afforded by the e-Privacy Directive so as to ensure that the rights of citizens, in particular those pertaining to the protection of users against targeting, are protected;
35. Requests that the Commission audit the activities of the advertising industry on social media and propose legislation in the event that the sector and concerned parties are unable to reach agreement on voluntary Codes of Conduct with dissuasive measures;
36. Calls on the data protection authorities at national and European level to undertake a thorough investigation into Facebook and its current practices so that the new consistency mechanism of the GDPR can be relied upon to establish an appropriate and efficient European enforcement response;
37. Calls on the Member States to take measures to address the risks posed to the security

¹ https://edps.europa.eu/sites/edp/files/publication/16-11-07_guidelines_web_services_en.pdf

of network and information systems used for the organisation of elections;

38. Takes the view that Member States should engage with third parties, including media, online platforms and information technology providers, in awareness-raising activities aimed at increasing the transparency of elections and building trust in the electoral process;
39. Is of the opinion that Member States should urgently conduct, with the support of Eurojust if necessary, investigations into the alleged misuse of the online political space by foreign powers;
40. Instructs its President to forward this resolution to the Council, the Commission, the governments and parliaments of the Member States and the United States of America, the Council of Europe and the CEO of Facebook.