YOUNG EUROPEAN FEDERALISTS

JEF Europe | Young European Federalists Brussels, 6th March 2016

The Human Right for Privacy in the Digital Age

Resolution submitted by: *JEF Political Commission 2 – Internal European Policy*

In an increasingly digitalized Europe, citizens' rights to their personal data is under threat. In recent years, news about government agencies' data sharing of their citizens or private companies' sketchy privacy policies that push its users for more data disclosure are alarming developments. JEF Europe asks Member States and EU institutions to recognize data privacy as an integral part of human rights paradigm and to implement stricter measures in the protection of its citizens' privacy.

JEF Europe,

A. *Wholeheartedly embracing* technological progresses to serve our society;
B. *Underlining* that;
    a. The right to privacy is a fundamental human right, as enshrined in the Charter of Fundamental Rights of the European Union, Art. 8;
    b. Major international documents such as the Universal Declaration of Human Rights (Art. 12), International Covenant on Civil and Political Rights (Art. 17), Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data of Council of Europe, while refer to the protection of personal data, are not sufficient under the current circumstances brought on by the increasing technological developments;
    c. Breaches on digital privacy are not only realized by states and their institutions, but also by non-state actors such as individuals, corporations and intergovernmental organizations;
C. *Fully aware* that the procedure of mass collection, combination and analysis of data, the so-called Big Data, allows for localisation, image- and voice-recognition and biometrics, and the collection and possible misuse of it is realized both by state and non-state actors;
D. *Emphasising* on the one hand, that these techniques of data collection possess great potential for the European industry, as well as for the democracy in Europe;

E. *Deeply disturbed,* on the other hand, about the possible and present massive abuse of these techniques by legal and illegal means, such as numerous tapping incidents at EU institutions, of political leaders and journalists, carried out by intelligence services, constituting a serious danger to European citizens, democracy and the industry as it results in the comprehensive profiling and complete encroaching of the individual;

F. *Noting* that information about people's preferences and opinions can be used as means of manipulation or even blackmailing by state institutions, corporations and individuals;

G. *While observing* that companies which have access to user data, such as Facebook and Google, base their business strategies on analysis and marketing of collected user data, also noting with deep concern that these automated analyses can be linked with the individual, resulting in the misuse of personalised advertising and cases of discrimination;

H. *Alarmed by the fact* that though this discriminatory practice often constitutes a breach of national data protection laws, companies can circumvent this by being based in another EU Member State with weak data protection legislation;

I. *Realising* that neither do users have the full means to understand the practice of collecting and marketing user data, nor do they have the possibility to defend themselves against it without having a professional know-how. Thus assuming that the personal responsibility lies with the users proves to be farfetched;

J. *Emphasising* that often the user has no information on alternative platforms and are inclined to submit their personal data due to the popularity of these mainstream platforms, as the search-engine, social-network, book-trading and hardware-production market is dominated by North American and Asian corporations. This is particularly worrying because of the often close cooperation between the intelligence services and the data industry, such is the case in the USA and China;

K. *Recalling* that many European states have suffered tremendously under totalitarian state surveillance;

L. *Deeply convinced* that European citizens should not only be the chief decision-makers on the control of their personal information but also should have the means

to take better decisions when acting in the digital sphere through enhancing consumer protection and information;

M. Critically *observing* that the US-led Five Eyes-system and European intelligence have built a broad surveillance infrastructure, nearly dissolving the fundamental human right of private sphere under the pretence of anti-terror protection, violating the right of private life (Art.7), the protection of personal data (Art. 8 and Art.16 Par. 1) and the freedom of speech (Art. 11, "chilling effect");

N. *While welcoming* the European Court of Justice's decision to repeal the Safe Harbour Agreement to transmit personal information within the transatlantic partnership, to improve the privacy standards for such exchanges, voices concern about the declaration of the European Commission to replace the agreement through a subsequent agreement named "EU-US-Privacy Shield" which just contains minimal further improvements in the protection of data privacy;

O. *Guided* by the conviction that a European federation can only be built on the basis of democracy, respect for human rights, and subsidiarity;

JEF Europe, therefore;

1. *Calls* Member States as well as EU institutions to recognise the human right of privacy as non-negotiable;

2. *Asks* Member States as well as EU-institutions to further the protection of freedom of speech and thought, especially with regards to the General Data Protection Regulation (GDPR) to harmonise their measures of data protection and even further improve the legislative

3. *Demands* accountability on the work of intelligence agencies, clearer identification of the risks of sharing personal data and transparency regarding the methods employed for collecting data, preventing future events like the tapping incidents, through full parliamentarian oversights competencies;

4. *Calling upon* the EU Member States and their partners to engage in a dialogue in order to stop mutual surveillance activities;

YOUNG EUROPEAN FEDERALISTS

5. *Demands* the European Commission to treat privacy as a fundamental rights issue and to continue for a uniform and strict European data protection legislation to protect EU citizens forcing not only national but also international companies to adhere to privacy regulation;

6. *Encourages*, therefore, the creation of an EU based privacy agency and support to the European Ombudsman and to ensure the abidance of EU laws protecting the human right to privacy, while ensuring the best cooperation possible with the already existing National Privacy Agencies;

7. *Calls*, thus, upon companies to make information as well as privacy settings and legal information about data usage easily accessible, hence empowering European users- to use the full democratic potential of digital means without being exploited;

8. *Recommends* that surveillance and collections of data, wiretappings or investigation undertaken by responsible authorities must be subject to a judicial procedure which guarantees individual freedoms;

9. *Further recommends* the Commission to adhere to the rules and regulations on critical communication infrastructures and inter-mediation platforms where privacy-issues persist and cannot be solved in the long-term;

Notes in conclusion that through these suggested means, Europe should eventually become a role model in promoting human rights for privacy in the digital age.