



EUROPEAN PARLIAMENT

2009 - 2014

Committee on Foreign Affairs

2012/2094(INI)

24.8.2012

DRAFT REPORT

on a Digital Freedom Strategy in EU Foreign Policy
(2012/2094(INI))

Committee on Foreign Affairs

Rapporteur: Marietje Schaake

CONTENTS

	Page
MOTION FOR A EUROPEAN PARLIAMENT RESOLUTION	3
EXPLANATORY STATEMENT.....	11

MOTION FOR A EUROPEAN PARLIAMENT RESOLUTION

on a Digital Freedom Strategy in EU Foreign Policy (2012/2094(INI))

The European Parliament,

- having regard to the resolution of the UN Human Rights Council of 5 July 2012 entitled ‘The promotion, protection and enjoyment of human rights on the Internet’, which recognises the importance of human rights protection and the free flow of information online,¹
- having regard to the reports of the UN Special Rapporteur Frank La Rue, of 16 May 2011 (A/HRC/17/27) and 10 August 2011 (A/66/290), on the promotion and protection of the right to freedom of opinion and expression, which underline the applicability of international human rights norms and standards regarding the right to freedom of opinion and expression on the internet, seen as a communications medium,
- having regard to the resolution of the UN Human Rights Council of 28 March 2008 (7/36) establishing the mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression,
- having regard to the UN report of 16 June 2011 entitled ‘Guiding Principles on Business and Human Rights: Implementing the United Nations ‘Protect, Respect and Remedy’ Framework’ (reflecting the work of UN Special Representative John Ruggie),
- having regard to the Strategic Framework on Human Rights and Democracy, adopted by the Council on 25 June 2012,²
- having regard to its recommendation to the Council of 13 June 2012 concerning the EU Special Representative for Human Rights³,
- having regard to its resolution of 12 June 2012 entitled ‘Critical information infrastructure protection – achievements and next steps: towards global cyber-security’⁴,
- having regard to its resolution of 20 April 2012 entitled ‘A competitive digital single market – eGovernment as a spearhead’⁵,
- having regard to its resolution of 18 April 2012 on the Annual Report on Human Rights in the World and the European Union’s policy on the matter, including implications for the EU’s strategic human rights policy⁶,
- having regard to the 2012 General Budget of 29 February 2012, in particular the call for

¹ <http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session20/Pages/ResDecStat.aspx>.

² http://eeas.europa.eu/delegations/un_geneva/press_corner/focus/events/2012/20120625_en.htm.

³ Texts adopted, P7_TA(2012)0250.

⁴ Texts adopted, P7_TA(2012)0237.

⁵ Texts adopted, P7_TA(2012)0140.

⁶ Texts adopted, P7_TA(2012)0126.

creating a ‘Global Internet Freedom Fund’¹,

- having regard to the communication of 12 December 2011 by the Commissioner for the Digital Agenda on the ‘No Disconnect Strategy’,
- having regard to the joint communication of the High Representative of the Union for Foreign Affairs and Security Policy and the European Commission to the European Parliament and the Council of 12 December 2011 entitled ‘Human Rights and Democracy at the Heart of EU External Action – Towards a more effective approach’ (COM(2011)0886)),
- having regard to its resolution of 17 November 2011 on the open Internet and net neutrality in Europe²,
- having regard to the Commission communication of 25 October 2011 entitled ‘A renewed EU strategy 2011-2014 for Corporate Social Responsibility’ (COM(2011)0681),
- having regard to its resolution of 25 July 2011 on an effective raw materials strategy for Europe³,
- having regard to its resolution of 7 July 2011 on EU external policies in favour of democratisation⁴,
- having regard to the Joint Communication of the High Representative of the Union for Foreign Affairs and Security Policy and the Commission of 25 May 2011 entitled ‘A new response to a changing Neighbourhood’ (COM(2011)0303),
- having regard to its resolution of 12 May 2011 on the cultural dimensions of the EU’s external actions⁵,
- having regard to its resolution of 25 November 2010 on corporate social responsibility in international trade agreements⁶,
- having regard to its resolution of 15 June 2010 entitled ‘Internet governance: the next steps’⁷,
- having regard to its resolution of 15 June 2010 on the Internet of Things⁸,
- having regard to its resolution of 14 February 2006 on the human rights and democracy clause in European Union agreements⁹,

¹ OJ L 56, 29.2.2012, p.1.

² Texts adopted, P7_TA(2011)0511.

³ Texts adopted, P7_TA(2011)0364.

⁴ Texts adopted, P7_TA(2011)0334.

⁵ Texts adopted, P7_TA(2011)0239.

⁶ OJ C 99E , 3.4.2012, pp. 101–111.

⁷ OJ C 236E , 12.8.2011, pp. 33-40.

⁸ OJ C 236E , 12.8.2011, pp. 24–32.

⁹ OJ C 290E , 29.11.2006, pp. 107–113.

- having regard to its resolutions on urgent cases of breaches of human rights, democracy and the rule of law, where they raise concerns regarding digital freedoms,
 - having regard to its legislative resolution of 27 September 2011 on the proposal for a regulation of the European Parliament and of the Council amending Regulation (EC) No 1334/2000 setting up a Community regime for the control of exports of dual-use items and technology¹,
 - having regard to Council Regulation (EU) No 36/2012 concerning restrictive measures in view of the situation in Syria and repealing Regulation (EU) No 442/2011 of 18 January 2012 and introducing export restrictions on ICTs and monitoring tools²,
 - having regard to Council Regulation (EU) No 264/2012 of 23 March 2012 amending Regulation (EU) No 359/2011 concerning restrictive measures directed against certain persons, entities and bodies in view of the situation in Iran and introducing export restrictions on ICTs and monitoring tools³,
 - having regard to Articles 3 and 21 of the Treaty on the Functioning of the European Union,
 - having regard to Article 207 of the Treaty on the Functioning of the European Union,
 - having regard to the European Union’s Guidelines on Human Rights,
 - having regard to the Universal Declaration of Human Rights and to all relevant international human rights instruments, including the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights,
 - having regard to the United Nations Charter,
 - having regard to the European Convention on Human Rights and the ongoing negotiations on the EU’s accession to the Convention,
 - having regard to the Charter of Fundamental Rights of the European Union,
 - having regard to Rule 48 of its Rules of Procedure,
 - having regard to the report of the Committee on Foreign Affairs and the opinion of the Committee on International Trade (A7-0000/2012),
- A. whereas technological developments enable individuals all over the world to use new information and communication technologies (ICTs) and to connect to the internet, thus fostering revolutionary changes in societies, the functioning of democracy, governance, the economy, business, media, development and trade;
- B. whereas internet access is a key enabler of access to information, free expression, press

¹ P7_TA(2011)0406.

² OJ L 16, 19.1.2012, p.1.

³ OJ L 86, 24.3.2012, p. 26.

freedom, freedom of assembly, and economic, social, political and cultural developments;

- C. whereas human rights need to be protected and promoted by the EU, both offline and online;
- D. whereas inclusion, the fostering of e-skills, and bridging digital divides are key in harnessing the empowering potential of the internet and ICTs;
- E. whereas ICTs are also used as tools of repression through (mass) censorship, surveillance, and tracing and tracking of information and individuals;
- F. whereas the context in which technologies are used determines, to a great extent, the impact they can have as a force for positive developments or for repression instead;
- G. whereas the internet has flourished and developed organically as a platform of huge public value;
- H. whereas the global and borderless nature of the internet requires new forms of international cooperation and governance with multiple stakeholders;
- I. whereas net neutrality is an essential principle for the open internet, ensuring competition and transparency;
- J. whereas digital security and digital freedom are both essential and cannot replace one another;
- K. whereas the EU only leads by example on digital freedoms when these are safeguarded in the EU;

Human rights and development

1. Recognises that uncensored access to the internet, mobile phones and ICTs have impacted on human rights and fundamental freedoms, exerting an enabling effect, by expanding the scope of freedom of expression, access to information, the right to privacy and freedom of assembly across the world;
2. Recognises the vast enabling, creating and catalysing potential of the internet and ICTs for global economic, social, scientific, cultural and political development, contributing as such to the progress of humankind as a whole;
3. Stresses that the repression and control of citizens and business involves a growing technological component, through the blocking of content and the monitoring and identification of human rights defenders, journalists, activists and dissidents, as well as through the criminalisation of legitimate expression online and the adoption of restrictive legislation to justify such measures;
4. Stresses that the promotion and protection of digital freedoms should be mainstreamed and annually reviewed so as to ensure accountability and continuity, in all the EU's external actions, financing and aid policies and instruments;

5. Reaffirms the Commission's recognition of unrestricted access to the internet as part of the Copenhagen criteria;
6. Encourages the EU Special Representative for Human Rights to name digital freedoms and the 'No Disconnect Strategy' among his key priorities;
7. Stresses that effective EU development policies require mainstreaming ICTs and bridging the digital divide, by providing basic technological infrastructures and facilitating access to knowledge and information;
8. Considers ICTs to be enablers of transparency and good governance, literacy, education, sexual and reproductive healthcare, effective election monitoring and disaster relief in remote areas or rural societies;
9. Stresses that EU development and aid programmes should include digital freedoms, above all in societies going through post-conflict or political transitions; believes that EU regulatory experts are essential interlocutors for purposes of training counterparts and embedding basic rights and principles in new (media) regulation and legislation;
10. Stresses that the digital collection of evidence and dissemination of images of human rights violations can contribute to the global fight against impunity; considers that assistance is needed in making materials admissible under international (criminal) law as evidence in court proceedings;
11. Emphasises the need to ensure that rare earth materials used in the production of ICTs are obtained in conditions of respect for human, labour and environmental rights;

Trade

12. Deplores the use of EU-made technologies and services in third countries to violate human rights through censorship of information, mass surveillance, monitoring, and the tracing and tracking of citizens and their activities on (mobile) telephone networks and the internet;
13. Welcomes the ban on the export of repression technologies and services to Syria and Iran; believes this ban should become a precedent for structural restrictive measures, such as an EU-wide 'catch-all' provision or 'country-specific lists' in the dual-use regulatory framework;
14. Underlines the need for more stringent supply-chain controls and corporate responsibility schemes in respect of trading in products (from equipment to mobile devices) and services which can be used to curtail human rights and digital freedom;
15. Regards certain targeted jamming, surveillance, monitoring and interception technology products and services as 'single-use' items whose export should be subject to ex ante approval;
16. Stresses the need to monitor EU sanctions on technologies at Union level so as to ensure that Member States comply equally and the level playing field is preserved;

17. Believes companies should perform human rights impact assessments on ICTs, starting at the R&D phase, and ensure non-complicity in possible human rights violations in third countries;
18. Calls on the Commission to provide EU businesses with a wide range of information and guidance, based on the UN's 'Ruggie Principles', so as to ensure that business interests and corporate social responsibility can be complied with;
19. Stresses the need to consider the effect of technological standard-setting for ICT and telecom products and services in the EU, where such goods and services are exported to third countries where concepts such as 'lawful interception' have different implications, for example where the rule of law does not exist;
20. Recognises that the internet has become a public space as well as a marketplace, for which the free flow of information and access to ICTs are indispensable;
21. Calls for the inclusion of conditionality clauses in EU FTAs, stipulating transparent safeguards, preserving unrestricted access to the internet, and ensuring the free flow of information;
22. Calls on the EU to challenge and minimise the extraterritorial impact of third-country legislation on EU citizens and businesses online;
23. Considers restricted access for EU businesses and online consumers to (digital) markets through mass censorship in third countries to constitute protectionist measures and trade barriers;
24. Calls on the EU to strive to ensure that regulation of the internet and ICTs is kept to the minimum;
25. Calls for the inclusion of targeted repression technologies in the Wassenaar Arrangement;

Internet governance

26. Considers transparent and collaborative decision-making to be essential to ensure respect for the open and participatory nature of the internet; believes the EU should play a leading role in the development of digital freedom ground-rules, including dispute settlement mechanisms, also taking account of conflicting jurisdictions;
27. Considers that the internet is currently relatively unregulated and is governed through a multi-stakeholder approach; stresses the need for the EU to ensure that the multi-stakeholder model is inclusive and that small businesses as well as civil society actors and users are not overruled by a few large business and government players;
28. Stresses the importance of an overall EU strategy for internet governance, as also for issues related to telecom regulation, which is internationally governed through the International Telecom Union, in which EU Member States each have one vote;
29. Is concerned at the proposals by coalitions of governments and business seeking to introduce regulatory oversight and increased governmental and private control over the

internet and telecom operations;

30. Recalls that the internet, data connection and storage and ICTs are essential parts of the EU's critical infrastructure;
31. Calls on the Commission to propose a new regulatory framework for e-commerce, as well as an update of the Intellectual Property Rights Enforcement Directive (IPRED), which would balance the need for copyright reform and protection with the need to protect fundamental rights online and preserve the open internet and would serve as a basis for IPR provisions and commitments in future FTAs;

A digital freedom strategy

32. Recognises that human rights must also be protected online, and believes ICTs should be mainstreamed in all EU programmes to advance this effort;
33. Calls on the Commission and Council to unequivocally recognise digital freedoms as fundamental rights and as indispensable prerequisites for enjoying universal human rights such as freedom of expression, freedom of assembly and access to information and ensuring transparency and accountability in public life;
34. Calls on the Commission and Council to support, train and empower human rights defenders, civil society activists and independent journalists and ensure their security and freedom online, and to assert the fundamental rights of free expression, freedom of assembly and freedom of association online;
35. Calls on the Commission and Council to upgrade their in-house ICT knowledge base;
36. Calls for political and diplomatic support for digital freedoms in recipient countries of EU aid, in addition to assistance programmes;
37. Considers that governments which restrict digital freedoms should become ineligible for EU aid, while those receiving EU aid should be required to use ICTs in order to increase transparency and accountability;
38. Urges the Council and Commission to include, in accession negotiations, human rights dialogues, trade negotiations and all forms of contact relating to human rights, conditionality clauses stipulating the need to respect and preserve unrestricted access to the internet, digital freedoms and human rights online;
39. Calls on the Commission and Council to promote and preserve high standards of digital freedom in the EU, in particular by codifying the principle of net neutrality in appropriate regulation, so as to strengthen its credibility in terms of promoting and defending digital freedoms around the world;
40. Considers that synergising the EU's trade, security and foreign policies and aligning its values and interests are indispensable if the Union is to fully leverage its economic power and act as a global player in defending digital freedoms;
41. Instructs its President to forward this resolution to the Council, the Commission and the

EEAS.

EXPLANATORY STATEMENT

Digital Freedom in the EU's External Actions

Internet and new technologies play an exponentially important role in the lives of Europeans and citizens everywhere. Globally technologies are changing societies, the functioning of our democracies, economies, businesses, media, development strategies, security and defence concerns and human rights issues. Information and power monopolies that have been unchallenged for a long time are upset.

Several EU Member States have identified access to internet as a fundamental right, and the European Commission agrees digital freedoms are part of the Copenhagen criteria. In a globally connected world the EU should have a strategy to deal with new technologies in its external actions. There are several areas in this digital world in which it is essential that the EU acts as a global player and leverages its economic and political weight. Though overregulation would rather hurt than help the potential of the open internet, in some areas rules need to be updated to match the revolutionary impact of technological developments with adequate democratic oversight.

This explanatory statement supports the draft of the first EU's Digital Freedom Strategy in its External Actions. A discussion paper has been shared with Members of European Parliament and was placed online to invite various stakeholders to provide input through crowd-sourcing. The input provided by many different people, NGOs, governments and businesses have helped the creation of the first draft to be more comprehensive. The Rapporteur is grateful to all who spent time and energy on each of these contributions.

Security and freedom

New technologies challenge the way in which governments perform their core tasks. Defence and security ultimately lie in the hands of government; however, these increasingly rely on private players. This requires new forms of cooperation and shared responsibilities. Given the importance of developing detailed cyber and digital security details, the rapport drafted by Rapporteur Kelam in the SEDE committee focuses on security. This report suggests a strategy dealing with EU human rights, development, enlargement, internet governance, trade, culture and diplomacy efforts.

Freedom and security need each other and can not replace one another. The European Parliament should ensure there is no zero sum game between the two, especially when it comes to digital and cyber issues. Given the EU's common security and defence policy as well as its economic interests, we should lead globally in securing both digital security and freedom.

Human rights

A quick scan of some events in the world shows that the struggle for human rights has moved online. Prisons are increasingly populated by dissidents confronted with their own internet

and mobile communications, compromised by the authorities. Iran continues the building of an electronic curtain, which eventually will cut off the Iranians from the World Wide Web through the creation of a 'Halal internet'. China is similarly cutting its citizens off of the open internet with the great electronic firewall. Mass censorship violates citizen rights and narrows business opportunities. Plans are on the table to make anonymous blogging in China illegal. The Ben Ali government of Tunisia was, and the Al Assad regime in Syria is well known for their sophisticated use of technologies against citizens. The Syrian Electronic Army is now subject to ad hoc EU sanctions.

Generally speaking, the fight for control and power by authoritarian regimes involves a growing ICT component. Promoting and defending human rights then means enabling people to circumvent mass censorship or to evade cyber attacks by their own governments. While training human rights defenders, journalists and dissidents should improve their safety online it also creates a new set of sensitivities and a potentially dangerous dependency on the accuracy and quality of the guidance. This responsibility should not be underestimated and has to be reflected in the ways and means we use to assist people in ensuring their freedom and safety online. Human rights defenders deserve EU support and in any case should not be targeted with tools and technologies developed and exported from within the EU.

Trade and export

Besides ad hoc export restrictions and trade sanctions regarding intrusive monitoring tools, the digital and globally connected reality calls for awareness and responsibility in European corporate boardrooms. It also requires comprehensive and permanent export restrictions to limit the harmful potential of sophisticated, targeted technology systems. Technologies, tools or services custom made for targeted human rights violations should not be allowed on European markets at all. These systems should be categorised as 'single use' technologies and do not differ from traditionally banned torture tools or (parts of) weapons of mass destruction in their impact.

While the recent EU export bans on certain elements of technologies to Syria and Iran are an important first step, they risk becoming a paper reality, threatening the EU's credibility, and the safety of citizens who think they can rely on the EU's efforts and promises. Instead of leaving enforcement up to the different member states, the European Commission should have the powers and tools to monitor the proper implementation of these restrictions. Transparency and accountability are needed in this field, much the same as we verify the quality of foods and medicine, or conventional weapons. This requires new policies such as non-financial disclosure requirements and updated reporting standards.

Additionally, the European Commission should help companies, in doubt whether to file for an export license, with real time information about the legality or potential harmful effects of trade deals. The same goes for EU (based) companies that enter into contractual relations with third country governments, whether to win operating licenses, negotiate standstill clauses or by accepting public involvement in business operations or public use of their networks and services, and which could force these businesses becoming complicit in human rights violations. Therefore the EU should make the conclusion of new free trade agreements conditional on the preservation of the open internet, or to provide ad hoc (public) political backing in emergency situations.

The changing balance of global powers and the emergence of a global economy means challenges to EU values when businesses operate abroad will occur more often and require joint efforts with European policymakers and civil society actors.

Development

The EU should make its development policies more efficient and effective through embracing ICTs. The EU can help bridge the digital divide; by building and installing basic ICT infrastructures and by providing access to knowledge and information. The EU can enable (online) education in remote areas by developing and providing cheap wirelessly connected tablets, allowing parents to let their children go to school. In the first critical hours after natural disasters or during humanitarian crisis ad hoc emergency telephone and internet connections should be set up. ICTs are also essential for effective (citizen) election monitoring.

Development programmes should therefore include the protection of digital freedoms in a structural way, in particular by planting seeds in early post-conflict or political transitions. EU regulators or regulatory experts should engage with their counterparts. Embedding basic rights principles in new (media) legislation is an essential safeguard and should prevent the inclusion of provision in laws that for instance make encryption illegal, such as currently in Egypt. These laws can have unintended effects on human rights that newly or (first time) elected parliaments or governments are not necessarily aware of.

The internet and particularly social media also enable governments to engage in direct diplomacy and allow increased people-to-people contact around the world. Open debates about ideas can refute extremism and improve intercultural engagement and understanding. The European Parliament should commit itself to including new technologies in the work of its delegations with other parliaments across the globe, and will keep a close watch on the progress and concrete measures taken to devise an EU strategy on digital freedom in its external relations. A proposed assessment in annual reports should ensure accountability and continuity.

Credibility

The EU can not credibly promote and protect digital freedoms in the world if they are not safeguarded at home. Although restrictions to freedom online sometimes are formally lawful there is also an overarching impact on our credibility and moral standing in the world. More pressingly, the same tools and technologies that our governments and law enforcement agencies can use to (lawfully) intercept mobile or internet traffic can have a fundamentally different impact on citizens in societies where the rule of law is absent or no separation of powers exists.

The European Commission is currently developing a set of human rights (and also broader corporate social responsibility) guidelines for the ICT sector, based on the UN Guiding Principles for Business & Human Rights (Ruggie principles). Whilst these guidelines will not legally bind European companies they might prove to be a useful framework for ICT companies in mainstreaming human rights concerns and in performing impact assessments,

even at the R&D phase or when filing for patents. These guidelines will also contribute to a level playing field in the EU's internal market.

Internet governance

The internet is governed by a so-called multi-stakeholder approach, which has been developed organically into a network of public and private actors. This approach has ensured the openness of the internet, which is the catalyst for many societal benefits. The multi-stakeholder model can only function properly when it is inclusive so that small businesses, users and consumers also have a seat at the table.

There are currently two threats to this system of governance. Developed countries are drafting legislation behind closed doors where only few corporate stakeholders have a say in the proceedings. Meanwhile the impact of proposed laws touches the very infrastructure of the internet. Largely below the radar, coalitions of emerging economies are joining forces to introduce a global regulatory framework for the internet, including increased state control and establishing an UN regulatory body. A new era of global internet politics has kicked off.

While the EU is the world's most significant market, most internet companies are US based, which forces European citizens to accept US user conditions. As most online services are US-based, internet users world-wide often fall within US jurisdiction when using these services. This extraterritorial impact of US laws should not restrain the EU's ability to defend the fundamental rights of citizens. Policymakers have to understand that in a globally connected world parameters of lawmaking are constantly changing and traditional concepts of set jurisdictions often do not match our global digital hemisphere. This however does not preclude the possibility of efficient dispute settlement mechanisms or addressing conflicting jurisdiction.

Digital Freedom Strategy

Our digital freedoms are essential rights and are indispensable for traditional human rights such as freedom of expression and freedom of assembly, and also for ensuring transparency and accountability in public life. We all see the impact of human rights violations that can be documented and shared with the help of mobile phones. The EU should take the lead in globally promoting and protecting digital freedoms. Besides being the world's largest trade block the EU is also a community of values, which should also be the core of all our external actions.

Only by synergising our trade, security and foreign policies, by aligning our values and interests the EU can fully leverage its power and act as a global player. As technology is developing so rapidly it is essential to promote structural collaboration between politicians, business and civil society. This ongoing equilibrium may best serve the open global internet, to everyone's benefit.