



EUROPEAN PARLIAMENT

2014 - 2019

Plenary sitting

A8-0000/2015

28.5.2015

REPORT

on ‘Human rights and technology: the impact of intrusion and surveillance systems on human rights in third countries’
(2014/2232(INI))

Committee on Foreign Affairs

Rapporteur: Marietje Schaake

CONTENTS

	Page
MOTION FOR A EUROPEAN PARLIAMENT RESOLUTION	3

MOTION FOR A EUROPEAN PARLIAMENT RESOLUTION

on ‘Human rights and technology: the impact of intrusion and surveillance systems on human rights in third countries’ (2014/2232(INI))

The European Parliament,

- having regard to the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, in particular Article 19 thereof,
- having regard to the European Union’s Strategic Framework on Human Rights and Democracy, adopted by the Council on 25 June 2012¹,
- having regard to the EU Human Rights Guidelines on Freedom of Expression Online and Offline, adopted by the Council (Foreign Affairs) on 12 May 2014²,
- having regard to the ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights, published by the European Commission in June 2013,
- having regard to the report by the Organisation for Security and Co-operation in Europe (OSCE) of 15 December 2011 entitled ‘Freedom of Expression on the Internet’³ and to the regular report of the OSCE Special Representative on Freedom of the Media to the OSCE Permanent Council of 27 November 2014⁴,
- having regard to the report of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, 23 September 2014 (A/69/397)⁵,
- having regard to the report of the Office of the UN High Commissioner for Human Rights of 30 June 2014 entitled ‘The right to privacy in the digital age’⁶,
- having regard to the report of the UN Special Rapporteur on the right to freedom of expression and opinion of 17 April 2013 (A/HRC/23/40) on the implications of states’ surveillance of communications on the exercise of the human rights to privacy and to freedom of opinion and expression,
- having regard to the report of the Committee on Legal Affairs and Human Rights of the Parliamentary Assembly of the Council of Europe of 26 January 2015 on ‘Mass surveillance’⁷,

¹ http://eeas.europa.eu/delegations/un_geneva/press_corner/focus/events/2012/20120625_en.htm.

² http://eeas.europa.eu/delegations/documents/eu_human_rights_guidelines_on_freedom_of_expression_online_and_offline_en.pdf.

³ <http://www.osce.org/fom/80723?download=true>.

⁴ <http://www.osce.org/fom/127656?download=true>.

⁵ <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N14/545/19/PDF/N1454519.pdf?OpenElement>.

⁶ http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A-HRC-27-37_en.doc.

⁷ <http://website-pace.net/documents/19838/1085720/20150126-MassSurveillance-EN.pdf/df5aae25-6cfe-450a->

- having regard to its resolution of 12 March 2014 on the United States National Security Agency surveillance programme, surveillance bodies in various EU Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs¹,
- having regard to the report by the Special Representative of the UN Secretary-General on human rights and transnational corporations and other business enterprises, of 21 March 2011, entitled 'Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework'²,
- having regard to the OECD guidelines for Multinational Enterprises³ and the 2014 annual report on the OECD guidelines for Multinational Enterprises⁴,
- having regard to the Internet Corporation for Assigned Names and Numbers Annual Report 2013⁵,
- having regard to the communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of 12 February 2014 entitled 'Internet Policy and Governance: Europe's role in shaping the future of Internet Governance'⁶,
- having regard to the NETmundial Multistakeholder Statement adopted on 24 April 2014⁷,
- having regard to the Chair's summary of the ninth Internet Governance Forum held in Istanbul on 2-5 September 2014,
- having regard to the European Union restrictive measures in place, some of which include embargoes on telecommunications equipment, information and communication technologies (ICTs) and monitoring tools,
- having regard to EU Regulation EU no 599/2014 of the European Parliament and of the Council of 16 April 2014 amending Council Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items⁸,
- having regard to the Joint Statement by the European Parliament, the Council and the

92a6-e903af10b7a2.

¹ Text adopted P7_TA(2014)0230.

²

http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf?v=1392752313000/_/jcr:system/jcr:versionstorage/12/52/13/125213a0-e4bc-4a15-bb96-9930bb8fb6a1/1.3/jcr:frozensnode

³ <http://www.oecd.org/daf/inv/mne/48004323.pdf>

⁴ <http://www.oecd-ilibrary.org/docserver/download/2014091e.pdf?expires=1423160236&id=id&accname=ocid194994&checksum=D1FC664FBCEA28FC856AE63932715B3C>

⁵ <https://www.icann.org/en/system/files/files/annual-report-2013-en.pdf>

⁶ COM(2014)0072.

⁷ <http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf>

⁸ OJ L 173, 12.6.2014.

Commission on the review of the dual-use export control system of 16 April 2014¹,

- having regard to the decisions of the 19th Plenary Meeting of the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies held in Vienna on 3-4 December 2013,
- having regard to the communication from the Commission to the Council and the European Parliament of 24 April 2014 entitled ‘The review of export control policy: ensuring security and competitiveness in a changing world’²,
- having regard to the Council Conclusions of 21 November 2014 on the review of export control policy,
- having regard to its resolution of 11 December 2012 on a Digital Freedom Strategy in EU Foreign Policy³,
- having regard to its resolution of 13 June 2013 on the freedom of the press and media⁴,
- 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 resolution of 12 March 2015 on the EU’s priorities for the UN Human Rights Council in 2015,
- having regard to its resolution of 11 February 2015 on the renewal of the mandate of the Internet Governance Forum⁵
- having regard to its resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens’ fundamental rights,
- having regard to its resolution on the Annual Report on Human Rights and Democracy in the World 2013 and the European Union’s policy on the matter⁶
- having regard to Edward Snowden’s written statement to the LIBE Committee of March 2014,
- 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 52 of its Rules of Procedure,
- having regard to the report of the Committee on Foreign Affairs (A8-0000/2015),

¹ OJ L 173, 12.6.2014.

² COM(2014)0244.

³ Texts adopted, P7_TA(2012)0470.

⁴ Texts adopted, P7_TA(2013)0274.

⁵ Texts Adopted, P8_TA(2015)0033.

⁶ Texts Adopted, P8_TA(2015)0076.

- A. whereas technological developments and access to the open internet are important for ensuring the fulfilment and full respect for human rights and fundamental freedoms, exerting a positive effect by expanding the scope of freedom of expression, access to information, the right to privacy and freedom of assembly and association across the world;
- B. whereas technological systems can be misused as tools for human rights violations through censorship, surveillance, unauthorised access to devices, jamming, interception, tracing and tracking of information and individuals;
- C. whereas this is done by public and private actors, including governments and law enforcement bodies, as well as criminal organisations and terrorist networks to violate human rights;
- D. whereas the context in which ICTs are designed and used determines, to a great extent, the impact they can have as a force to advance or to violate human rights, information technology, especially software is rarely single-use and usually dual-use as far as their potential to violate human rights is concerned, while software also is a form of speech;
- E. whereas ICTs have been key instruments in organizing social movements and protest in various countries, especially under authoritative regimes;
- F. whereas the assessment of the context is determined by the strength of national and regional legal frameworks to regulate the use of technologies and the ability of political and judicial institutions to oversee such use;
- G. whereas in the digital domain, private actors play an increasingly significant role in all spheres of social activities, but safeguards are still not in place to prevent them from imposing excessive restrictions on fundamental rights and freedoms; as a result, private actors play a more active role in assessing the legality of content and in developing cyber security systems and surveillance systems, which can have a detrimental impact on human rights all over the world;
- H. whereas the Internet represents a revolution in terms of the possibilities for exchanging data, information and knowledge of all kinds;
- I. whereas encryption is an important method that helps to secure communications and the people using them;
- J. whereas internet governance has benefitted from a multistakeholder decision making model; a process ensuring meaningful, inclusive and accountable participation of all stakeholders, governments, civil society, technical and academic communities, private sector, and users;
- K. whereas intelligence agencies have systematically undermined cryptographic protocols and products in order to be able to intercept; whereas the US National Security Agency has collected vast numbers of so called 'zero-day exploits' – IT security vulnerabilities that are not yet known to the public or the product vendor; whereas such activities undermine global efforts to improve IT security;

- L. whereas EU-based intelligence services have engaged in activities that harm human rights;
 - M. whereas in light of rapid technological developments, judicial and democratic oversight and safeguards are largely underdeveloped;
 - N. whereas (cyber-)security and counter-terrorism measures involving ICTs, or the monitoring of the internet can have a significant detrimental effect on the human rights and individual freedoms of people all over the world, including EU citizens when residing or travelling abroad, and especially in the absence of legal basis, necessity, proportionality or democratic and judicial oversight;
 - O. whereas internet filters and communication surveillance undermine human rights defenders' ability to take advantage of the Internet and to communicate sensitive information, and are in breach of several articles in the Universal Declaration of Human Rights (UDHR) guaranteeing every person's rights to privacy and freedom of expression;
 - P. whereas digital security and digital freedom are both essential and cannot replace one another, but should reinforce one another;
 - Q. whereas the European Union can only lead by example on digital freedoms when these are safeguarded in the EU itself, and thus adopting the EU data protection package is crucial;
 - R. whereas far-reaching social interests are at stake, such as the protection of fundamental rights, which should not be determined by the market alone, but need regulation,
 - S. whereas respect for fundamental rights and the rule of law and effective parliamentary oversight of intelligence services using digital surveillance technology are important elements of international cooperation;
 - T. whereas EU-based companies have an important share of the global market in ICTs, in particular when it comes to exporting surveillance, tracking, intrusion and monitoring technology;
 - U. whereas the introduction of export controls should not harm legitimate research into IT security issues and the development of IT security tools without criminal intent;
1. Recognises that human rights and fundamental freedoms are universal and need to be defended globally in every dimension of their expression; stresses that the surveillance of communications, as such, interferes with the rights to privacy and expression, if conducted outside an adequate legal framework;
 2. Calls on the Commission to ensure coherence between the EU's external actions and its internal policies related to ICTs;
 3. Believes that mass surveillance of citizens and the spying on political leaders by the US NSA with the active complicity of certain EU Member States, as revealed by Edward

Snowden, have caused serious damage to the credibility of the EU's human rights policy and have undermined global trust in the benefits of ICTs;

4. Reminds the Member States and EU agencies, including Europol and Eurojust, of their obligations under the Charter of Fundamental Rights of the European Union, international human rights law and of the EU's external policy objectives, which forbid them to share intelligence data which might lead to human rights violations in a third country or to use information obtained as a result of a human rights violation, such as unlawful surveillance, outside the EU;
5. Stresses that the impact of technologies on the improvement of human rights should be mainstreamed in all EU policies and programmes, if applicable, to advance human rights protection and the promotion of democracy, rule of law and good governance as well as peaceful conflict resolution;
6. Calls for the active development and dissemination of technologies that help protect human rights and facilitate people's digital rights and freedoms as well as their security, along with promoting best practices and appropriate legislative frameworks, while guaranteeing the security and the integrity of personal data; in particular, urges the EU and its Member States to promote the global use and development of open standards and free and open-source software and cryptographic technologies;
7. Calls on the EU to increase its support for actors, those who work on strengthening security and privacy protection standards in ICTs on all levels, including hardware, software and communication standards as well as the development of the hardware and software in privacy-by-design frameworks;
8. Calls for a human rights and technology fund to be established under the European Instrument for Democracy and Human Rights;
9. Urges the EU itself, and in particular the EEAS, to use encryption in its communications with human rights defenders, to avoid putting defenders at risk and to protect its own communications with outsiders from surveillance;
10. Calls on the EU to adopt free and open source software as well as to encourage other actors to do so, as such software provides for better security and for greater respect for human rights;
11. Draws attention to the importance of developing ICTs in conflict areas to promote peacebuilding activities with a view to providing secure communication between parties involved in peaceful resolution of conflicts;
12. Calls on the implementation of the conditions, benchmarks and reporting procedures in order to ensure that the EU financial and technical support to the development of new technologies in third countries is not used in a way that infringes human rights;
13. Calls on the Commission and the Council to actively engage with third country governments, and to further support, train and empower human rights defenders, civil society activists and independent journalists using ICTs in their activities in a safe

manner, by means of the existing European support mechanisms and policy instruments, and to promote related fundamental rights of privacy, such as the unrestricted access to information on the internet, the right to privacy and data protection, freedom of expression, freedom of assembly, freedom of association and freedom of the press and publication online;

14. Draws attention to the plight of whistleblowers and their supporters, including journalists following their revelations of abusive surveillance practices in third countries; believes that such individuals should be considered as human rights defenders and therefore that they deserve the protection by the EU as required under the EU Guidelines on Human Rights Defenders; reiterates its call on the Commission and the Member States to thoroughly examine the possibility of granting whistleblowers international protection from prosecution;
15. Deplores that security measures, including counterterrorism measures, are increasingly used as pretexts for the violation of the right to privacy and for clamping down on the legitimate activities of human rights defenders, journalists and political activists; reiterates its strong belief that national security can never be a justification for untargeted, secret or mass surveillance programmes; insists that such measures be pursued strictly in line with rule of law and human rights standards, including the right to privacy and data protection;
16. Calls on the EEAS and the Commission to promote the democratic oversight of security and intelligence services in its political dialogue with third countries as well as in its development cooperation programmes; urges the Commission to support civil society organizations and legislative bodies in third countries aiming at enhancing scrutiny, transparency and accountability of domestic security services; calls for specific commitments thereon to be included in the future EU Action Plan on Human Rights and Democratisation;
17. Urges the Council and the Commission to promote digital freedoms and unrestricted access to the internet in all forms of contact with third countries, including in accession negotiations, trade negotiations, human rights dialogues and diplomatic contacts;
18. Recognizes 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; therefore stresses that digital freedom and free trade must be promoted and protected simultaneously;
19. Calls for the inclusion of clauses in all agreements with third countries which explicitly refer to the need to promote, guarantee and respect digital freedoms, net neutrality, uncensored and unrestricted access to the internet, privacy rights and the protection of data;
20. Urges the EU to counter the criminalisation of human rights defenders' use of encryption, censorship-bypassing and privacy tools, by refusing to limit the use of encryption within the EU and challenge third country governments which use such charges against defenders;

21. Urges the EU to counter the criminalisation of the use of encryption, anti-censorship and privacy tools, by refusing to limit the use of encryption within the EU, and by challenging third country governments which criminalise such tools;
22. Stresses that an effective EU development and human rights policy will require the mainstreaming of ICTs and the bridging of the digital divide, by providing basic technological infrastructure and facilitating access to knowledge and information to promote digital skills and the use of open standards in documents as well as the use of free and open source software, where appropriate, for openness and transparency (especially by public institutions), and including the safeguarding of data protection in the digital realm all over the world, as well as a better understanding of the potential risks and benefits of ICTs;
23. Calls on the Commission to support the elimination of digital barriers for people with disabilities; considers it extremely important that EU policies on development and the promotion of human rights in the world should aim to mitigate the digital divide for people with disabilities and to provide a broader framework of rights, particularly as regards access to knowledge, digital participation and inclusion in new economic and social opportunities created by the internet;
24. Underlines that the lawful digital collection and dissemination of evidence of human rights violations can contribute to the global fight against impunity and terrorism; considers that such material should be admissible, in duly justified cases under international (criminal) law as evidence in court proceedings, in line with international, regional and constitutional safeguards; and recommends that mechanisms be created in the field of international criminal law for the introduction of procedures through which such data is authenticated and collected for use as proof in court proceedings;
25. Deplores the fact that some of the EU-made information and communication technologies and services are sold and can be used in third countries by private individuals, businesses and authorities to specifically violate human rights through censorship, mass surveillance, jamming, interception, monitoring, and the tracing and tracking of citizens and their activities on (mobile) telephone networks and the internet; is concerned with the fact that some EU-based companies may provide the technologies and services which may, in turn, lead to these human rights violations;
26. Notes that threats to the security of the European Union, its Member States and to third countries, often come from individuals or small groups using digital communication networks to plan and carry out attacks, and that the tools and tactics required to defeat such threats need to be constantly reviewed and updated;
27. Considers mass surveillance that is not justified by a heightened risk from terrorist threats to be in violation of the principles of necessity and proportionality, and, therefore, a violation of human rights;
28. Urges Member States to promote full democratic scrutiny over the operations of intelligence services in third countries, and that these services operate in full respect of the rule of law, and to hold to account those who are responsible for operating in unlawful ways;

29. Encourages Member States, in the light of the increased cooperation and exchange of information between Member States and third countries - including through the use of digital surveillance - to ensure democratic scrutiny of those agencies and their activities through appropriate internal, executive, judicial and independent parliamentary oversight;
30. Stresses that corporate social responsibility principles and human rights by design criteria, which are technological solutions and innovations protecting human rights, should be adopted in EU law to ensure that internet service providers, software developers, hardware producers, social networking services/media, mobile phone carriers and others consider the human rights of end-users globally;
31. Urges the EU to ensure greater transparency in the relationship between mobile phone carriers or ISPs and governments, and to call for it in its relations with third countries, by demanding that carriers and ISPs publish yearly detailed transparency reports, including reports on requested actions by authorities, as well as financial ties between public authorities and carriers/ISPs;
32. Reminds corporate actors of their responsibility to respect human rights throughout their global operations regardless of where its users are located and independently of whether the host state meets its own human rights obligations; calls on ICT companies, notably EU-based ones, to implement the UN Guiding Principles on Business and Human Rights, including through establishing due diligence policies and risk management safeguards and providing effective remedies when their activities have caused or contributed to an adverse human rights impact;
33. Stresses the need to more effectively implement and monitor EU regulations and sanctions relating to ICTs, including the use of catch-all mechanisms, so as to ensure that all parties, including Member States, comply with legislation and that a level playing field is preserved;
34. Stresses the fact that respect for fundamental rights is an essential element in successful counter-terrorism policies, including the use of digital surveillance technologies;
35. Welcomes the December 2013 Wassenaar Arrangement decision on export controls in the areas of surveillance, law enforcement and intelligence gathering tools and network surveillance systems; recalls the still very incomplete nature of the EU dual-use regime, namely the EU dual-use regulation, when it comes to the effective and systematic export control of harmful ICT technologies to non-democratic countries;
36. Urges the Commission, in the context of the forthcoming dual-use policy review and renewal, to swiftly put forward a proposal for smart and effective policies to limit and regulate the commercial export of services regarding the implementation and use of so-called dual-use technologies, addressing potentially harmful exports of ICT products and services to third countries, as agreed in the Joint Statement of the European Parliament, Council and Commission of April 2014; calls on the Commission to include effective safeguards to prevent any harm of these export controls to research, including scientific and IT security research;

37. Stresses that the Commission should be able to swiftly and accurately provide companies that are in doubt as to whether to apply for an export licence with up-to-date information on the legality or potentially harmful effects of potential transactions;
38. Calls on the Commission to submit proposals to review how EU standards on ICTs could be used to prevent the potentially harmful impacts of the export of such technologies or other services to third countries where concepts such as 'lawful interception' cannot be considered equivalent to those of the European Union, or for example have a poor record on human rights, or where the rule of law does not exist;
39. Reaffirms that EU standards, particularly the EU Charter of Fundamental Rights, should prevail when assessing incidents when dual-use technologies are used in a way that may restrict human rights;
40. Calls for the development of policies to regulate the sales of zero-day exploits and vulnerabilities to avoid their being used for cyber-attacks or for unauthorised access to devices leading to human rights violations without such regulations having a meaningful impact on academic and otherwise bona fide security research;
41. Deplores the active co-operation of certain European companies, as well as international companies which trade dual-use technologies with potential detrimental effects on human rights while operating in the EU, with regimes whose actions violate human rights;
42. Urges the Commission publicly to exclude companies engaging in such activities from EU procurement procedures, from research and development funding and from any other financial support;
43. Calls on the Commission to pay particular attention to human rights aspects in the public procurement processes for technological equipment, especially in countries with unreliable practises in this domain;
44. Calls on the Commission and Council to actively defend the open internet, multi-stakeholder decision-making procedures, net neutrality, digital freedoms and data protection safeguards in third countries through internet governance fora;
45. Condemns the weakening and undermining of encryption protocols and products, particularly by intelligence services who wish to intercept communications that are encrypted;
46. Warns against the privatization of law enforcement through internet companies and internet service providers;
47. Calls for a clarification of norms and standards that private actors use to develop their systems;
48. Recalls the importance of assessing the context within which technologies are used, in order to fully appreciate their human rights impact;

49. Explicitly calls for promoting tools enabling the anonymous and/or pseudonymous use of the internet and to challenge the one-sided view that such tools are allowing criminal activities, rather than empowering human rights activists beyond and within the EU;
50. Urges the Council, the Commission and the External Action Service to develop smart and effective policies to regulate the export of dual-use technologies, addressing potentially harmful exports of ICT products and services, at international level within multilateral export control regimes and other international bodies;
51. Stresses that any regulatory changes aimed at increasing the effectiveness of export controls vis-à-vis Intangible Technology Transfers must not inhibit legitimate research and access to and exchange of information, and that any potential measures such as the use of EU General Export Authorisations for dual-use research should not have a 'chilling effect' upon individuals and SMEs;
52. Calls on Member States to ensure that existing and future export control policies do not restrict the activities of legitimate security researchers, and that export controls are applied in good faith to only clearly defined technologies intended to be used for mass surveillance, censorship, jamming, interception, monitoring, and the tracing and tracking of citizens and their activities on (mobile) telephone networks;
53. Recalls that mesh-based ad hoc wireless technologies offer a high potential to provide for backup networks in areas where the internet is unavailable or blocked, and can help the advancement of human rights;
54. Calls on the Commission to appoint an independent group of experts who can perform a human rights impact assessment on existing EU standards for ICTs, with the goal of making recommendations for adjustments that will increase the protection of human rights, particularly when systems are exported;
55. Recognises that technological development poses a challenge to legal systems which need to adjust to new circumstances; further underlines the importance of law makers paying more attention to issues relating to the digital economy;
56. Calls on the Commission to involve civil society, and independent experts, including security researchers, in the ICT field in third countries, to ensure up-to-date expertise that should result in future-proof policy making;
57. Underlines the need to avoid unintended consequences such as restrictions or chilling effects on scientific and other types of bona fide research and development, on the exchange of and access to information and the development of security knowledge or on the export of technologies that are in the interest of acquiring the requisite digital skills and advancing human rights;
58. Believes that cooperation between governments and private actors worldwide in the digital domain calls for clear checks and balances and must not lead to the undermining of democratic and judicial oversight, including the Internet Governance Forum;
59. Notes that a voluntary approach is not enough, and that binding measures are required

to encourage companies to take into account a country's human rights record before selling their products there and to carry out an assessment of the effect their technologies will have on human rights defenders and government critics;

60. Is of the opinion that the export of highly sensitive goods must be checked before these highly sensitive goods leave the EU and that penalties are necessary in the event of violations;
61. Calls for each individual to be entitled to encryption and also for the necessary conditions to be created to be able to operate encryption; takes the view that controls should be a matter for the end user who will need the skills required to carry out such controls properly;
62. Calls for the introduction of 'end to end' encryption standards as a matter of course for all communication services so as to make it more difficult for governments, intelligence agencies and surveillance bodies to read content;
63. Emphasises the special responsibility of government intelligence services to build trust and calls for an end to mass surveillance; considers that the monitoring of European citizens through domestic and foreign intelligence services has to be addressed and stopped;
64. Is opposed to the sale and distribution of European surveillance technology and censorship tools to authoritarian systems in which the rule of law does not exist;
65. Calls for the scope for international protection of whistleblowers to be extended and also encourages Member States to table laws to protect them;
66. Calls for a UN envoy for digital liberties and data protection to be appointed and calls for the brief of the EU commissioner for human rights to be extended so that technology is also considered from a human rights angle;
67. Calls for measures to ensure that the privacy of activists, journalists and citizens is protected everywhere in the world and that they are able to network via the Internet;
68. Insists on the right to Internet access as a human right and calls for measures to eliminate the digital divide;
69. Instructs its President to forward this report to the Council, the Commission, the Vice-President of the Commission / High Representative of the Union for Foreign Affairs and Security Policy, and the EEAS.

RESULT OF FINAL VOTE IN COMMITTEE

Date adopted	26.5.2015
Result of final vote	+: 33 -: 6 0: 24
Members present for the final vote	Lars Adaktusson, Petras Auštrevičius, Amjad Bashir, Goffredo Maria Bettini, Mario Borghezio, Elmar Brok, Klaus Buchner, James Carver, Javier Couso Permuy, Mark Demesmaecker, Georgios Eptideios, Eugen Freund, Michael Gahler, Richard Howitt, Sandra Kalniete, Tunne Kelam, Afzal Khan, Janusz Korwin-Mikke, Andrey Kovatchev, Eduard Kukan, Ilhan Kyuchyuk, Ryszard Antoni Legutko, Arne Lietz, Barbara Lochbihler, Sabine Lösing, Ramona Nicole Mănescu, David McAllister, Francisco José Millán Mon, Javier Nart, Pier Antonio Panzeri, Demetris Papadakis, Vincent Peillon, Alojz Peterle, Tonino Picula, Andrej Plenković, Cristian Dan Preda, Jozo Radoš, Sofia Sakorafa, Jacek Saryusz-Wolski, Alyn Smith, Jaromír Štětina, Charles Tannock, Eleni Theoharous, László Tőkés, Ivo Vajgl, Boris Zala
Substitutes present for the final vote	Bodil Ceballos, Ignazio Corrao, Tanja Fajon, Andrzej Grzyb, Marek Jurek, Jo Leinen, Javi López, Antonio López-Istúriz White, Fernando Maura Barandiarán, Norbert Neuser, Urmas Paet, Godelieve Quisthoudt-Rowohl, Marietje Schaake, György Schöpflin
Substitutes under Rule 200(2) present for the final vote	Damian Drăghici, Maria Grapini, Josef Weidenholzer