



EUROPEAN PARLIAMENT

2014 - 2019

---

*Plenary sitting*

---

**A8-0178/2015**

3.6.2015

# 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

	<b>Page</b>
MOTION FOR A EUROPEAN PARLIAMENT RESOLUTION.....	3
RESULT OF FINAL VOTE IN COMMITTEE.....	16

## 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 2012<sup>1</sup>,
- having regard to the EU Human Rights Guidelines on Freedom of Expression Online and Offline, adopted by the Council (Foreign Affairs) on 12 May 2014<sup>2</sup>,
- having regard to the ‘ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights’, published by the 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’<sup>3</sup> and to the regular report of the OSCE Special Representative on Freedom of the Media to the OSCE Permanent Council of 27 November 2014<sup>4</sup>,
- 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)<sup>5</sup>,
- 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’<sup>6</sup>,
- having regard to the report of the UN Special Rapporteur of 17 April 2013 on the right to freedom of expression and opinion (A/HRC/23/40), analysing 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’<sup>7</sup>,

---

<sup>1</sup> [http://eeas.europa.eu/delegations/un\\_geneva/press\\_corner/focus/events/2012/20120625\\_en.htm](http://eeas.europa.eu/delegations/un_geneva/press_corner/focus/events/2012/20120625_en.htm).

<sup>2</sup> [http://eeas.europa.eu/delegations/documents/eu\\_human\\_rights\\_guidelines\\_on\\_freedom\\_of\\_expression\\_online\\_and\\_offline\\_en.pdf](http://eeas.europa.eu/delegations/documents/eu_human_rights_guidelines_on_freedom_of_expression_online_and_offline_en.pdf).

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

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

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

<sup>6</sup> [http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A-HRC-27-37\\_en.doc](http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A-HRC-27-37_en.doc).

<sup>7</sup> <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 Affairs<sup>1</sup>,
- 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’<sup>2</sup>,
- having regard to the OECD guidelines for Multinational Enterprises<sup>3</sup> and the 2014 annual report on the OECD guidelines for Multinational Enterprises<sup>4</sup>,
- having regard to the Internet Corporation for Assigned Names and Numbers Annual Report 2013<sup>5</sup>,
- 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’<sup>6</sup>,
- having regard to the NETmundial Multistakeholder Statement adopted on 24 April 2014<sup>7</sup>,
- 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 force, 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 items<sup>8</sup>,
- having regard to the Joint Statement by the European Parliament, the Council and the

---

92a6-e903af10b7a2.

<sup>1</sup> Text adopted, P7\_TA(2014)0230.

<sup>2</sup>

[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:frozennode](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:frozennode)

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

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

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

<sup>6</sup> COM(2014)0072.

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

<sup>8</sup> OJ L 173, 12.6.2014.

Commission on the review of the dual-use export control system of 16 April 2014<sup>1</sup>,

- 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’<sup>2</sup> ,
- 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 Policy<sup>3</sup> ,
- having regard to its resolution of 13 June 2013 on the freedom of the press and media<sup>4</sup>,
- 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<sup>5</sup>,
- having regard to its resolution of 11 February 2015 on the renewal of the mandate of the Internet Governance Forum<sup>6</sup>
- 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<sup>7</sup>,
- 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 matter<sup>8</sup>,
- having regard to Edward Snowden’s written statement to the LIBE Committee of March 2014<sup>9</sup>,
- having regard to the European Convention on Human Rights and the ongoing negotiations on the EU’s accession to the Convention,

---

<sup>1</sup> OJ L 173, 12.6.2014.

<sup>2</sup> COM(2014)0244.

<sup>3</sup> Texts adopted, P7\_TA(2012)0470.

<sup>4</sup> Texts adopted, P7\_TA(2013)0274.

<sup>5</sup> Texts adopted, P8\_TA(2015)0079.

<sup>6</sup> Texts adopted, P8\_TA(2015)0033.

<sup>7</sup> Texts adopted, P7\_TA(2014)0230.

<sup>8</sup> Texts adopted, P8\_TA(2015)0076.

<sup>9</sup>

<http://www.europarl.europa.eu/document/activities/cont/201403/20140307ATT80674/20140307ATT80674EN.pdf>.

- 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 (A8-0178/2015),
- A. whereas technological developments and access to the open internet are playing an increasingly important role in enabling and 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, and the 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 violate – human rights; whereas information technology, especially software, is rarely single-use and usually dual-use as far as the potential to violate human rights is concerned, while software is also a form of speech;
  - E. whereas ICTs have been key instruments helping people organise social movements and protests in various countries, especially in countries with authoritative regimes;
  - F. whereas the assessment of the implications for human rights of the context in which technologies will be used 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; whereas, 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 it offers 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 multi-stakeholder decision-making model, a process ensuring meaningful, inclusive and accountable participation of all

stakeholders, including governments, civil society, technical and academic communities, the private sector and users;

- K. whereas intelligence agencies have systematically undermined cryptographic protocols and products in order to be able to intercept communications and data; whereas the US National Security Agency (NSA) has collected vast numbers of so called ‘zero-day exploits’, that is, 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 the light of the rapid technological developments that are taking place, judicial and democratic oversight and safeguards are largely underdeveloped;
- N. whereas (cyber-)security and counter-terrorism measures involving ICTs, and 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 a legal basis that rests on the precepts of necessity, proportionality, and democratic and judicial oversight;
- O. whereas internet filters and communication surveillance undermine the ability of human rights defenders 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 each person’s right to privacy and to 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, when it comes to digital freedoms, the European Union can only lead by example when these freedoms are safeguarded in the EU itself; and whereas adopting the EU data protection package is therefore crucial;
- R. whereas what is at stake are far-reaching social interests – such as the protection of fundamental rights – that should not be determined by the market alone, and that 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, or the development of IT security tools, where there is no 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 the active complicity of certain EU Member States in the NSA's mass surveillance of citizens and spying on political leaders, as revealed by Edward Snowden, has caused serious damage to the credibility of the EU's human rights policy and has undermined global trust in the benefits of ICTs;
4. Reminds the Member States and the EU agencies concerned, including Europol and Eurojust, of their obligations under the Charter of Fundamental Rights of the European Union, and in keeping with international human rights law and with the EU's external policy objectives, not to share intelligence data that may lead to human rights violations in a third country, nor to use information obtained by means of human rights violations, 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 the protection of human rights and the promotion of democracy, the rule of law and good governance, and 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, and that promote best practices and appropriate legislative frameworks, while guaranteeing the security and integrity of personal data; urges, in particular, the EU and its Member States to promote the global use and development of open standards, and of free and open-source software and cryptographic technologies;
7. Calls on the EU to increase its support for actors who work on strengthening security and privacy protection standards in ICTs at all levels, including hardware, software and communication standards, as well as on developing 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, and 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 for the implementation of conditions, benchmarks and reporting procedures so as to ensure that EU financial and technical support to the development of new technologies in third countries is not used in ways that infringe on human rights;
13. Calls on the Commission and the Council to engage actively 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 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 human rights defenders and that, as such, they deserve the EU's protection, as required under the EU Guidelines on Human Rights Defenders; reiterates its call on the Commission and the Member States to examine thoroughly the possibility of granting whistleblowers international protection from prosecution;
15. Deplores the fact that security measures, including counterterrorism measures, are increasingly used as pretexts for violations 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 the 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 organisations and legislative bodies in third countries that seek to enhance the 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. 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; stresses, therefore, 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 that refer explicitly 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 to challenge third-country governments that level such charges against human rights 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 that 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, by facilitating access to knowledge and information to promote digital skills, and by promoting the use of open standards in documents and the use of free and open-source software, where appropriate, to ensure openness and transparency (especially by public institutions) – 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 the development of and promotion of human rights in the world should aim at mitigating 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 the 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; 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 EU-made information and communication technologies and services are sold, and can be used, in third countries by private individuals, businesses and authorities with the specific intent of violating human rights by means of censorship, mass surveillance, jamming, interception and monitoring, and by tracing and tracking citizens and their activities on (mobile) telephone networks and the internet; is concerned about the fact that some EU-based companies may provide technologies and services that can enable such human rights violations;
26. Notes that threats to the security of the European Union and 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 reviewed and updated constantly;

27. Considers mass surveillance that is not justified by a heightened risk of terrorist attacks and threats to be in violation of the principles of necessity and proportionality, and, therefore, a violation of human rights;
28. Urges the Member States to promote full democratic scrutiny of the operations of intelligence services in third countries, to verify that these services operate in full respect of the rule of law, and to hold to account those services and individuals operating in unlawful ways;
29. Encourages the Member States, in the light of the increased cooperation and information exchange between Member States and third countries (including through the use of digital surveillance), to ensure democratic scrutiny of these services, and of 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 (ISPs), 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 on 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 their users are located and independently of whether the host state meets its own human rights obligations; calls on ICT companies, notably those based in the EU, to implement the UN Guiding Principles on Business and Human Rights, including through the establishment of due diligence policies and risk management safeguards, and the provision of effective remedies when their activities have caused or contributed to an adverse human rights impact;
33. Stresses the need to implement and monitor EU regulations and sanctions relating to ICTs more effectively, including the use of catch-all mechanisms, so as to ensure that all parties, including the 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, swiftly to 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 swiftly be able to provide companies that are in doubt as to whether to apply for an export licence with accurate and up-to-date information on the legality or potentially harmful effects of potential transactions;
38. Calls on the Commission to submit proposals for a review of 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, that 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 in assessments of incidents involving dual-use technologies used in ways 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 of international companies trading in 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 actively to 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 seeking to intercept encrypted communications;
46. Warns against the privatisation of law enforcement through internet companies and ISPs;
  47. Calls for a clarification of the norms and standards used by private actors 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. Calls explicitly for the promotion of tools enabling the anonymous and/or pseudonymous use of the internet, and challenges the one-sided view that such tools serve only to allow criminal activities, and not to empower human rights activists beyond and within the EU;
  50. Urges the Council, the Commission and the EEAS 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 and within multilateral export control regimes and other international bodies;
  51. Stresses that any regulatory changes aimed at increasing the effectiveness of export controls of intangible technology transfers must not inhibit legitimate research, or 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' on individuals or SMEs;
  52. Calls on the 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, and only to clearly defined technologies intended to be used for mass surveillance, censorship, jamming, interception or monitoring purposes, or for tracing and tracking citizens and their activities on (mobile) telephone networks;
  53. Recalls that mesh-based, ad hoc wireless technologies offer great potential in providing 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 that 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, requiring them to adjust to new circumstances; underlines the importance of law makers paying more attention to issues pertaining to the digital economy;
  56. Calls on the Commission to involve civil society as well as 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, on the development of security knowledge or on the export of technologies that are in the interest of acquiring the requisite digital skills and of advancing human rights;
58. Believes that cooperation between governments and private actors worldwide in the digital domain, including the Internet Governance Forum, calls for clear checks and balances and must not lead to the undermining of democratic and judicial oversight;
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 they leave the EU, and that penalties are necessary in the event of violations;
61. Calls for each individual to be entitled to encryption, and for the conditions needed to allow encryption to be created; 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 must be addressed and stopped;
64. Is opposed to the sale and distribution of European surveillance technology and censorship tools to authoritarian regimes under which the rule of law does not exist;
65. Calls for the scope for international protection of whistleblowers to be extended, and encourages the Member States to table laws to protect whistleblowers;
66. Calls for a UN envoy for digital liberties and data protection to be appointed, and for the brief of the EU Commissioner for Human Rights to be extended, such 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 that internet access should be recognised 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

<b>Date adopted</b>	26.5.2015
<b>Result of final vote</b>	+: 33 -: 6 0: 24
<b>Members present for the final vote</b>	Lars Adaktusson, Petras Auštrevičius, Amjad Bashir, Goffredo Maria Bettini, Mario Borghezio, Elmar Brok, Klaus Buchner, James Carver, Javier Couso Permuy, Mark Demesmaecker, Georgios Epitideios, 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
<b>Substitutes present for the final vote</b>	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
<b>Substitutes under Rule 200(2) present for the final vote</b>	Damian Drăghici, Maria Grapini, Josef Weidenholzer