



Brugge

College of Europe
Collège d'Europe



Natolin

Democracy and Digital Authoritarianism: An Assessment of the EU's External Engagement in the Promotion and Protection of Internet Freedom

Susanna Garside



DEPARTMENT OF EU INTERNATIONAL
RELATIONS AND DIPLOMACY STUDIES

EU Diplomacy Paper

01 / 2020



College of Europe
Collège d'Europe

Brugge



Natolin

Department of EU International
Relations and Diplomacy Studies

EU Diplomacy Papers

1/2020

Democracy and Digital Authoritarianism: An Assessment of the EU's External Engagement in the Promotion and Protection of Internet Freedom

Susanna Garside

© Susanna Garside

About the Author

Susanna Garside was a recipient of the Denman Scholarship awarded by the Bruges-Natolin UK European Scholarships Fund (Brunat Fund), graduating in 2019 with an MA in EU International Relations and Diplomacy Studies from the College of Europe in Bruges. She also holds a BA in European Studies from Trinity College Dublin. She currently works for GIZ (Deutsche Gesellschaft für Internationale Zusammenarbeit) in Kampala as part of the EU co-funded Civil Society in Uganda Support Programme. This paper is based on her Master's thesis at the College of Europe (Manuel Marin Promotion).

Editorial Team:

Sara Canali, Bram De Botselier, Carsten Gerards, Sieglinde Gstöhl, Tatiana Kakara, Victor Le Grix, Simon Schunz, Oleksandra Zmiyenko

Dijver 11 | BE-8000 Bruges, Belgium | Tel. +32 (0)50 477 251 | Fax +32 (0)50 477 250 |
E-mail ird.info@coleurope.eu | www.coleurope.eu/ird

Views expressed in the *EU Diplomacy Papers* are those of the authors only and do not necessarily reflect positions of either the series editors or the College of Europe.

Abstract

The past decade has seen a gradual global increase in digital authoritarianism. Internet shutdowns, online censorship, mass surveillance and violations of privacy rights have all become more frequent in parts of the world where citizens are not guaranteed sufficient digital rights. The task of defending, promoting and protecting internet freedom is becoming increasingly relevant for the European Union (EU) – for internal digital and cybersecurity policies as well as for the EU’s external promotion of democracy and human rights. Whilst much has been written about the various internal policies which establish and protect internet freedom within the European Union and its member states, the EU’s external engagement in this field remains critically under-researched. To what extent does the EU engage externally in the promotion and protection of internet freedom? This paper answers this question by covering a wide variety of policy fields including human rights and democracy promotion, digital policy, enlargement and neighbourhood policy, development cooperation and trade policy. Whereas the EU faces a limited opportunity to shape global norms with regard to internet freedom or to change the course of digitally authoritarian states, it has demonstrated several strengths which deserve not to be overlooked. These include, for example, the externalisation of internal data protection and policies and the provision of direct support and protection for civil society. Despite facing significant obstacles, the promotion and protection of internet freedom has become an important area of the EU’s external action which is only set to become more relevant in the coming years.

Introduction: technology as a double edged-sword for democracy

*"Technology can support human rights, but we must also ensure it is not used against those struggling for freedom."*¹ – Neelie Kroes, 2011

The link between democracy and internet freedom is at the forefront of discussions over internet shutdowns, content regulation, disinformation, cybersecurity, online privacy and surveillance. The benefits of the internet as a precious tool for enabling transparency and increased democratic participation are widely understood and often taken for granted. However, the internet has also been increasingly presented as a threat to democracy and even as a tool which can enable forms of "postmodern totalitarianism".² Global internet freedom has been in decline over the past decade and elements of a dystopian future of cyberspace surveillance, control and manipulation somewhat akin to those in Orwell's '1984' are not far from reality in some of the more severe cases of digital authoritarianism.³ In a world with four billion internet users where internet penetration is increasing rapidly and 70% of the world's youth are online, issues of internet freedom are only set to become more prevalent in the future.⁴ Questions of whether and how controls for various aspects of internet governance should be implemented are now issues of growing geopolitical significance.

The task of defending, promoting and protecting internet freedom is becoming increasingly relevant in EU internal digital and cybersecurity policies as well as in the external promotion of democracy and human rights. Whilst much has been written about the various internal policies which establish and protect internet freedom within the European Union (EU) and its member states, the EU's external engagement in the promotion and protection of internet freedom remains critically under-researched.⁵ This paper will answer the question: to what extent does the EU engage externally in the promotion and protection of internet freedom. The paper argues that although the EU faces a limited opportunity to shape global norms with regard to internet

¹ Cited in: European Commission, "Digital Agenda: Karl-Theodor zu Guttenberg invited by Kroes to promote internet freedom globally", *Press Release*, Brussels, 12 December 2011.

² L. Diamond, "The Road to Digital Unfreedom: The Threat of Postmodern Totalitarianism", *Journal of Democracy*, vol. 30, no. 1, 2019, p. 20.

³ *Ibid.*, p. 21; Freedom House, *Freedom on The Net 2018*, Washington, D.C., 2018, p. 4.

⁴ Youth is defined as people aged 15-24 years. See: B. Sanou, "ICT Facts and Figures 2017", *International Telecommunication Union*, Geneva, 2017, p. 1.

⁵ At the time of writing, the only published research on the topic appears to be a 2013 report discussing the EU's role in promoting freedom of expression online. See: B. Pellot, "Index policy paper: Is the EU heading in the right direction on digital freedom?", *Index on Censorship*, 20 June 2013.

freedom or to change the course of digitally authoritarian states, it has demonstrated several strengths which deserve not to be overlooked. These include, for example, the externalisation of internal data protection and policies and the provision of direct support and protection for civil society.

The findings in this paper are based upon a combination of document- and interview-based research.⁶ As well as making use of the relevant academic literature and publicly available EU policy documents, a series of semi-structured interviews were conducted with representatives from the European Commission's Directorate-General for Communications Networks, Content and Technology (DG CONNECT), the Directorate-General for International Cooperation and Development (DG DEVCO) and from the European Endowment for Democracy (EED).

My research design purposefully encompasses many different areas of EU external engagement in an attempt to build a complete picture of EU external engagement in the field of the promotion and protection of internet freedom. It is therefore not within the scope of this work to take consideration of the individual and specific country contexts of EU external action. However, as the EU's engagement in this policy area continues to expand, this paper can serve as a useful point of reference for further research that could take a more specific country or regional focus. The research could also serve as a basis for further studies aiming to assess the impact of various elements of the EU's external engagement in this field.

After defining what is meant by the term 'internet freedom', the paper will discuss the value of the internet as a tool for strengthening democracy. Based upon this discussion, the following sections will look at the global institutional setting and global norm cleavages as well as the internal legal and policy frameworks for EU engagement in the promotion and protection of internet freedom. The EU's external engagement in this domain will then be analysed, looking into the policy fields of human rights and democracy promotion, digital policy, enlargement and neighbourhood policy, development cooperation and trade policy. This will offer

⁶ For more details see: S. Garside, *Democracy and Digital Authoritarianism: An Assessment of the EU's External Engagement in the Promotion and Protection of Internet Freedom*, Master's thesis, Bruges, College of Europe, 2019.

insights into the challenges faced as well as the identification of opportunities for further development of the EU's current approach.

What is meant by 'internet freedom'?

The term 'internet freedom' encompasses a broad range of interrelated human rights, often referred to as 'digital rights'. These include the rights to internet access, online freedom of expression, digital privacy and the right to seek, receive and impart information online.⁷ The question of whether internet access should itself be considered a human right has attracted considerable attention. Whilst many have argued that it does indeed constitute a human right, others rather see it as a tool which can be used to enable other rights.⁸ Regardless of which perspective is taken on the issue, the United Nations (UN) has clearly condemned any attempt to intentionally prevent or disrupt access to the internet and has stressed the need for human rights to underpin internet governance, stating that the rights people have offline must also be protected online.⁹

The rights to internet access, online freedom of expression, digital privacy and the right to seek, receive and impart information online are broadly encompassed within the UN Universal Declaration of Human Rights (UDHR). Under Article 19, individuals are entitled to freedom of opinion and expression, including the right to receive and impart information and ideas "through any media and regardless of frontiers", and Article 12 states that no individual shall be "subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation".¹⁰

As is conceived by Freedom House in their annual "Freedom on the Net" report, digital rights can be organised into three distinct categories: 'obstacles to access', 'limits on content' and 'violations of user rights'.¹¹ Obstacles to access includes infrastructural limitations and economic barriers to access, as well as government efforts to block or

⁷ J. Kurbalija, *An Introduction to Internet Governance*, DiploFoundation, Msida, 7th edn., 2016, p. 207.

⁸ V.G. Cerf, "Internet Access Is Not A Human Right", *The New York Times*, 4 January 2012.

⁹ United Nations, General Assembly, "The promotion, protection and enjoyment of human rights on the Internet", Resolution 32/13, 1 July 2016.

¹⁰ United Nations, General Assembly, *Universal Declaration of Human Rights*, Resolution 217 A (III), Paris, 1948.

¹¹ Freedom House, *Freedom on The Net 2018*, Washington, D.C., 2018, p. 24.

limit access.¹² Limits on content refer to forms of censorship and content manipulation, including the filtering and blocking of websites. This category also considers the diversity of online news media and the usage of digital media for purposes of social and political activism.¹³ Violations of user rights include restrictions on online activity, questions of privacy, anonymity and surveillance as well as repercussions for online activity, such as legal prosecution, imprisonment, physical attacks or other forms of harassment.¹⁴

These three elements of internet freedom can be seen as interdependent: obstacles to access and limits on content both dictate the value of freedom expression online, and freedom expression online itself depends on assurances of privacy and freedom from unwarranted surveillance. It is thus the combination of the three categories of 'obstacles to access', 'limits on content' and 'violations of user rights' which will underpin the understanding of internet freedom to be used in this paper.

The internet: a tool for strengthening democracy?

In the information age of the 21st century, discussions about democracy and media freedom can hardly be detached from issues of internet freedom and digital rights. Although it is clear that ICT is not in itself a solution for democracy, internet access does have important benefits to offer. In the academic debate, so-called 'cyber-enthusiasts' or 'techno-optimists' have highlighted the benefits of internet access as a tool for facilitating freedom of expression, lowering the costs of obtaining information, organising and contributing to collective action.¹⁵ Additionally, internet-based platforms present opportunities for increased transparency and accountability as well as opening the possibility for increased participation or even new forms of voting systems.¹⁶ For example, the concept of 'e-democracy', which is primarily based on models of participatory and deliberative democracy, refers to the use of online

¹² *Ibid.*

¹³ *Ibid.*

¹⁴ *Ibid.*

¹⁵ H. Margetts, "The Internet and Democracy", in W. Dutton (ed.), *The Oxford Handbook of Internet Studies*, Oxford, Oxford University Press, 2013, p. 1.

¹⁶ In Europe, recent years have seen populist movements – in particular Italy's Five Star Movement and Spain's Podemos – make first attempts at creating digital platforms to capitalise on the attraction of direct democratic involvement. See: F. Berti, "E-Politics for 'the people'? The case studies of Rousseau and Podemos", *The Good Lobby*, 27 September 2017.

platforms to support and enhance democratic functions.¹⁷ In a more general sense, it can also be argued that by enabling access to information and education, contributing to greater socio-economic equality or empowering women within communities, internet access also benefits democracy in more indirect ways.

However, in the context of a global trend of declining internet freedom, it is important to recognise that any benefits associated with the use of the internet as a tool for increased transparency, citizen engagement or activism remain conditional upon the insurance of sufficient internet freedom and digital rights. Worldwide, the adoption of cybersecurity measures has frequently been accompanied by deteriorations in internet freedom and the growing trend of disrespect for digital rights has even led some ‘cyber-sceptics’ and ‘techno-pessimists’ to argue that the internet now poses “a major threat to democratic stability and human freedom”.¹⁸

Internet shutdowns, which can be understood as obstacles to access caused by “intentional disruption of internet or cellphone networks in response to political or social events”, have become a more prevalent global phenomenon.¹⁹ Data collected and published by the advocacy group Access Now shows that the number of global shutdowns increased from 75 in 2016 to 188 in 2018 – with India listed as the worst offender.²⁰ Apart from the huge economic cost of internet shutdowns, blocking access to the internet restricts digital rights and can be seen as a form of antidemocratic government control which limits both access to information and freedom of expression.

Limitations on freedom of expression can also be seen where various governments have chosen to place limits on content by selectively restricting access, blocking certain internet sites and communication applications. Restrictions to social media access on election days has become common practice in many countries across Africa and several countries including China, Russia, Turkey and Iran have chosen to impose permanent bans on certain social media sites (such as Facebook, Twitter and

¹⁷ European Parliamentary Research Service, “Prospects for e-democracy in Europe: Study Summary”, Brussels, February 2018, p. 7.

¹⁸ Diamond, *op. cit.*, p. 20.

¹⁹ Freedom House, “Freedom on the Net Methodology”.

²⁰ Access Now, “Internet Shutdowns in Context: Insights from the Shutdown Tracker Optimization Project (STOP)”, 13 December 2018; Raw data obtained from Access Now, *op. cit.*

YouTube) or secure messaging services which allow users to send encrypted messages (such as Telegram, WhatsApp and Signal).²¹ In Uganda, the so-called 'over-the-top' social media tax has been criticised for limiting access for over 2.5 million users.²² Whilst some users manage to circumvent blocks using Virtual Private Networks (VPNs), governments – albeit some quicker than others – have begun to acquire VPN blocking technology and implement laws which render the use of VPNs illegal.²³

When it comes to violations of user rights, China is often used to illustrate some of the world's most extreme cases of censorship and digital rights violations.²⁴ The Chinese government operates the world's most advanced apparatus for internet censorship, known as the 'Great Firewall', which not only blocks access to tens of thousands of sites and domain names, but also enables automated and systematic internet censorship of content criticising the regime.²⁵ China has begun to assert its dominance in cyberspace through new measures to implement what can best be described as a "surveillance state".²⁶ A new cybersecurity law introduced in June 2017 compromises user anonymity by strengthening the existing obligation of internet companies to register users under their real names.²⁷ Limits on VPNs which help internet users to conceal their identity, location or nature of their activity are in place and Chinese companies are legally obliged to co-operate with the government in safeguarding national security.²⁸ This gives the Chinese government the ability to access large amounts of data, which is an essential element of the state's surveillance strategy. The forthcoming nationwide Social Credit System (SCS), which is due to be fully implemented by 2020, will encompass vast amounts of data tracking citizens' in-person and online behaviour.²⁹ Despite the fact that studies have shown high approval levels for the system amongst the Chinese public, with many considering the

²¹ T. Freyburg & L. Gabre, "Blocking the Bottleneck: Internet Shutdowns and Ownership at Election Times in Sub-Saharan Africa", *International Journal of Communication*, vol. 12, 2018, pp. 3896-3916.

²² R. Ratcliffe & S. Okiror, "Millions of Ugandans quit internet services as social media tax takes effect", *The Guardian*, 27 February 2019.

²³ A. O'Driscoll, "Where are VPNs legal and where are they banned?", *Comparitech*, 13 November 2017.

²⁴ Freedom House, *Freedom on The Net 2018*, *op. cit.*, p. 1.

²⁵ Freedom House, "China Country Report: Freedom on the Net 2018", 2018.

²⁶ X. Qiang, "The Road to Digital Unfreedom: President Xi's Surveillance State", *Journal of Democracy*, vol. 30, no. 1, 2019, pp. 53-67.

²⁷ Freedom House, "China Country Report: Freedom on the Net 2018", *op. cit.*

²⁸ *Ibid.*

²⁹ State Council of the People's Republic of China, *Planning Outline for the Construction of a Social Credit System (2014-2020)*, trans. R. Creemers, 14 June 2014.

rewards that high credit scores can offer, defenders of internet freedom have well-founded fears that the SCS will only reinforce and further substantiate limits to freedom of expression.³⁰ Considering that arrests and imprisonments of online activists already occur regularly in China, the SCS is likely to further limit citizens' abilities to express themselves freely online.³¹

Whilst obstacles to access and internet censorship create immediate challenges to media freedom and democracy, violations of user rights, including legal action and imprisonment of online journalists and activists, have created a double cause for concern – on the one hand, for the immediate rights of the affected individuals, and on the other, for the deterrent this causes for other citizens who no longer consider using the internet as a platform for exercising their right to freedom of expression.

Although the lowest ranking in the Freedom House internet freedom ranking are almost exclusively illiberal regimes, limitations to internet freedom are certainly not unique to these countries.³² Questions of internet freedom have increasingly reached headline news within liberal democracies, with most attention granted to issues of data privacy, cybersecurity and surveillance. Perhaps the most shocking revelation of breaches of internet freedom made in the context of any liberal democracy were those made by Edward Snowden in 2013 about the mass surveillance programmes of the National Security Agency (NSA) of the United States (US).³³ Snowden revealed that the NSA was able to tap directly into the servers of nine internet firms, including Facebook, Google, Microsoft and Yahoo, in order to track online communications.³⁴ This scandal demonstrated that the failure to balance security concerns and internet freedom was not only an issue in digitally authoritarian states. Snowden's revelations about violations of privacy committed by the UK's Government Communications Headquarters (GCHQ) showed that even within the EU, sufficient surveillance safeguards cannot always be counted on.³⁵

³⁰ G. Kostka, "China's Social Credit Systems and Public Opinion: Explaining High Levels of Approval", *New Media & Society*, vol. 21, no. 7, 2019, pp. 1565-1593.

³¹ Freedom House, "China Country Report: Freedom on the Net 2018", *op. cit.*

³² Freedom House, *Freedom on The Net 2018*, *op. cit.*, p. 25.

³³ BBC News, "Edward Snowden: Leaks that exposed US spy programme", 17 January 2014.

³⁴ *Ibid.*

³⁵ O. Bowcott, "GCHQ data collection regime violated human rights, court rules", *The Guardian*, 13 September 2018.

In 2018, the Facebook-Cambridge Analytica scandal brought considerable attention to the link between data privacy and democracy. The scandal which has since been described as “a lesson in institutional failure” revealed that the UK-based political consulting firm, Cambridge Analytica, had harvested personal data from millions of Facebook users without their consent and used the data to create targeted, politically-motivated communications and advertising strategies.³⁶ The data was used to support clients including Donald Trump’s presidential campaign and the Leave EU campaign in the UK.³⁷ The idea that the internet could be used as a communication tool for election campaigning is not a new one, but the revelations were the first to show the extent to which violations of internet users’ data privacy can have damaging effects on democracy.

Russian interference in the 2016 US presidential election which occurred “in sweeping and systematic fashion” drew further attention to the damage that the internet can cause to democracy.³⁸ As well as hacking computer networks belonging to Hilary Clinton’s campaign team, social media campaigns implemented the use of ‘troll farms’ – vast teams of operatives who create fake social media accounts in order to support particular opinions or spread disinformation and distrust.³⁹ Subsequent elections have been plagued with concerns regarding online disinformation and election-hacking.

The following section addresses the global institutional setting for internet governance as well as the global norm cleavages related to internet freedom. This will enable a better understanding of the EU’s opportunity for external engagement in the promotion and protection of internet freedom.⁴⁰

³⁶ C. Cadwalladr, “Cambridge Analytica a year on: ‘a lesson in institutional failure’”, *The Guardian*, 17 March 2019.

³⁷ *Ibid.*

³⁸ U.S. Department of Justice, “Report On The Investigation Into Russian Interference In the 2016 Presidential Election”, Washington, D.C., vol. 1, March 2018, p. 1.

³⁹ D. Lee, “The tactics of a Russian troll farm”, *BBC News*, 16 February 2018.

⁴⁰ This understanding of opportunity draws on C. Bretherton & J. Vogler, *The European Union as a Global Actor*, Abingdon, Routledge, 2006, 2nd edn, pp. 24-27.

Limited opportunity: challenges for the EU in a fragmented global setting

Whilst it is clear that the information age has brought with it numerous complex transboundary problems, internet governance remains characterised by a fragmented global institutional setting which is multi-stakeholder in nature.⁴¹ Internet governance encompasses a whole host of issues including Domain Name Systems (DNSs), accessibility, privacy, surveillance, intellectual property rights and cyber-security. Besides issues related to DNSs, which are managed through the non-profit, California-based Internet Corporation for Assigned Names and Numbers (ICANN), issues of internet governance are primarily addressed under the UN-convened Internet Governance Forum (IGF). The IGF brings together various stakeholder groups – including governments, private sector firms, civil society groups, members of the technical and academic community – in order to facilitate policy dialogue on issues of internet governance as equals.⁴² Although it facilitates exchange of best practice and offers a possibility for raising pressing issues related to internet governance, the IGF has been criticised for being a “mere talking shop”.⁴³ It remains a weak, but nonetheless important, international institution which serves as a forum for discussion, both reflecting and shaping the global norms and values surrounding internet freedom.

The EU attends the annual IGF conferences and is actively involved in the forum but does not have the same opportunity to exert influence in other international internet governance organisations. The Freedom Online Coalition (FOC) – an organisation made up of a set of thirty governments committed to supporting internet freedom and protecting human rights – is a state-based organisation which does not offer membership to regional organisations.⁴⁴ Fourteen of its thirty members, however, are EU member states.⁴⁵ In the case of the Global Network Initiative (GNI), a multi-stakeholder platform created to specifically address issues of internet censorship and online privacy by supporting companies in developing self-regulatory approaches, neither states nor regional organisations are invited to apply for membership.⁴⁶

⁴¹ L. Dendaris, *The Global War for Internet Governance*, New Haven, Yale University Press, 2014, p. 226.

⁴² Internet Governance Forum, “About the IGF”, n.d.

⁴³ C.M. Glen, *Controlling Cyberspace: The Politics of Internet Governance and Regulation*, Santa Barbara, CA, Praeger, 2018, p. 38.

⁴⁴ Freedom Online Coalition, “Freedom Online: Joint Action for Free Expression on the Internet [Founding Declaration]”, 15 December 2011.

⁴⁵ Freedom Online Coalition, “About Us: Members”, n.d.

⁴⁶ Global Network Initiative, “About”, n.d.

In the field of cybersecurity, all EU member states are signatories to the Council of Europe's Budapest Convention on Cybercrime.⁴⁷ The convention, which came into force in July 2004, covers *inter alia* the topic of violations of network security.⁴⁸ With 66 signatories, the international convention is a legally binding international instrument which establishes common domestic criminal legislation on cybercrime and fosters international co-operation.⁴⁹ However, the convention is limited by the fact that important global players such as Russia and China have not agreed to sign up. Furthermore, many of the existing signatories have recently expressed a need for the contents of the convention to be strengthened.⁵⁰

Alongside the structural context of internet and cybersecurity governance, it is also important to consider the global norms and institutions in place for governing the trade of surveillance technologies. ICT surveillance technologies are classified as 'dual-use' items, that is to say items which can be used for both civilian and military purposes. Examples include 'spyware' such as devices for mobile telecommunications interception, jamming equipment, Internet Protocol (IP) network surveillance systems and intrusion software.⁵¹ These technologies have been covered under the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and technologies since December 2013.⁵² The Wassenaar Arrangement promotes transparency and greater responsibility in transfers of dual-use goods and technologies.⁵³ Agreed guiding principles are implemented via national legislation and signatory states engage in established processes of information sharing.⁵⁴ The Arrangement currently has 42 participating states including Russia and the US and – with the exception of Cyprus (whose membership was blocked by Turkey) – all EU member states are signatories. Aside from the fact that the Wassenaar Arrangement is not an international treaty and is therefore not legally binding, the scope of the Arrangement

⁴⁷ Council of Europe, "Recommendation CM/Rec(2016)5 of the Committee of Ministers to member States on Internet freedom", 13 April 2016; Council of Europe, "Convention on Cybercrime", Budapest, 23 November 2001.

⁴⁸ Council of Europe, "Convention on Cybercrime", *op. cit.*

⁴⁹ Council of Europe Treaty Office, "Chart of signatures and ratifications of Treaty 185: Convention on Cybercrime", n.d.

⁵⁰ Implied within the Paris Call, see: France Diplomatie, Ministry for Europe and Foreign Affairs, "Paris Call for Trust and Security in Cyberspace", 11 December 2018.

⁵¹ M. Bromley *et al.*, "ICT Surveillance Systems: Trade Policy and the Application of Human Security Concerns", *Strategic Trade Review*, vol. 2, no. 2, 2016, p. 38.

⁵² *Ibid.*

⁵³ Wassenaar Arrangement, "About Us", n.d.

⁵⁴ *Ibid.*

is limited by its focus on concerns of international security and stability which often trump human rights concerns.⁵⁵ Furthermore, China, which has a booming export industry for ICT surveillance technologies and Artificial Intelligence (AI), is not a signatory.⁵⁶

Above and beyond the institutional settings for issues related to internet freedom, perhaps the most significant constraining factor in the EU's external environment is the global norm cleavage related to internet freedom – in particular regarding issues of privacy. Although under Article 12 of the UDHR the right to privacy is understood to be a universal right, it is clear that the right to privacy is not respected or interpreted in the same way across the globe. Digitally authoritarian states with low internet freedom ratings, such as China and Russia, have defended the concept of 'internet sovereignty' which favours strong national controls over the internet, opposing the EU and US view of an open and multi-stakeholder approach to internet governance. With China beginning to promote its model of cybersecurity to governments in South-East Asia, Africa and the Middle East, the universality of the right to privacy is endangered and the split in understandings over models for internet governance has created a challenging environment for promoting values of internet freedom.⁵⁷

In summary, it can be seen that the global institutional setting is very fragmented, with various organisations and institutions attempting to address a wide range of different topics. The existing multi-stakeholder approach – which is the approach favoured by the EU – purposefully rejects a strong, single regulatory body who could 'control the internet'. When it comes to cybersecurity and export controls for surveillance technologies, the overarching structures for international co-operation suffer from numerous limitations arising from both the scope of issues addressed and their lack of universal application. The deepening ideological split between those moving towards forms of digital authoritarianism and those favouring an open and free internet leaves very little opportunity for the EU to transform the nature of the global structural context. The following section will analyse the internal context of EU action, taking into account

⁵⁵ Bromley *et al.* argue that adding technologies to the Wassenaar Arrangement on purely human rights grounds would likely be opposed. See: Bromley *et al.*, *op. cit.*, p. 45.

⁵⁶ S.N. Romaniuk & T. Burgers, "How China's AI Technology Exports Are Seeding Surveillance Societies Globally", *The Diplomat*, 18 October 2018; Wassenaar Arrangement, *op. cit.*

⁵⁷ Freedom House reports on training seminars run by Chinese officials and suggests that various new cybersecurity and cybercrime laws have been modelled on those of China. See: Freedom House, *Freedom on The Net 2018*, *op. cit.*, p. 8.

the legal and policy frameworks surrounding EU policy-making in the promotion and protection of internet freedom.

Understanding the internal context of EU external action

The topic of internet freedom is not explicitly mentioned in the Treaties and the EU Charter of Fundamental Rights. However, building upon several articles which express the EU's legal commitment to upholding values of human dignity, democracy and respect for human rights, the topic has greater prominence in EU policy documents over time.⁵⁸ An explicit commitment to promoting and protecting internet freedom was presented in the 2012 Strategic Framework and Action Plan on Human Rights and Democracy.⁵⁹ This was further developed in the 2015 Action Plan on Human Rights on Democracy and, most notably, in the 2014 EU Human Rights Guidelines on Freedom of Expression Online and Offline (hereinafter referred to as the Guidelines).⁶⁰

Although their title may suggest an explicit focus on freedom of expression, the Guidelines in fact form the basis for much of the EU's external engagement in the promotion and protection of internet freedom, addressing a range of topics including privacy, surveillance and even public diplomacy.⁶¹ Despite not being legally binding in character, the Guidelines present an important point of reference for officials from the and its member states, for example during the delivery of technical assistance or in discussions of conditionality in human rights dialogues with third countries. The priority action areas covered by the Guidelines span many policy domains, including human rights and democracy promotion, digital policy, enlargement and neighbour-hood policy, international development and trade policy.⁶² This means that policy-making processes related to the promotion and protection of internet freedom rely on the co-operation of multiple actors, decision-making procedures and funding mechanisms.

⁵⁸ See Articles 2, 6, 21, 49 TEU and articles 7, 8, 10, 11, 22 of the EU Charter of Fundamental Rights in: European Union, "Consolidated Versions of the Treaty on European Union and the Treaty on the Functioning of the European Union of 13 December 2007", *Official Journal of the European Union*, C326, 16 October 2012.

⁵⁹ Council of the European Union, "EU Strategic Framework and Action Plan on Human Rights and Democracy", Luxembourg, 25 June 2012.

⁶⁰ Council of the European Union, "EU Action Plan on Human Rights and Democracy", Brussels, 20 July 2015; Council of the European Union, "EU Human Rights Guidelines on Freedom of Expression Online and Offline", Brussels, 12 May 2014.

⁶¹ *Ibid.*

⁶² *Ibid.*

In the field of digital policy and in the trade of dual-use technologies, the EU has – in accordance with the legal principles of subsidiarity and proportionality – gained some level of legal competence to create binding legislation. In development cooperation, which is a shared competence of the EU and its member states, the EU has the ability to use funding mechanisms such as the Development Cooperation Instrument (DCI) to develop initiatives which support the development of digital infrastructure. In the field of human rights and democracy promotion, the EU has a dedicated funding instrument, the European Instrument for Democracy and Human Rights (EIDHR), from which considerable funds are dedicated to internet freedom-related projects. For the candidate countries and the countries of the European Neighbourhood Policy (ENP), funding to support online freedom of expression and media plurality is delivered through the Instrument for Pre-Accession (IPA) and the European Neighbourhood Instrument (ENI). Further to this, the EU supports the work of the European Endowment for Democracy, a specialised agency which was established in 2013 to provide civil society support, primarily to neighbourhood countries.

One factor that has positively influenced the EU's agenda with regard to the promotion of internet freedom is the agenda-setting role of the European Parliament. Led by Marietje Schaake, a Dutch member of the Alliance of Liberals and Democrats for Europe Party (ALDE), the European Parliament has put forward a progressive agenda for the promotion of internet freedom. In 2012 it adopted a resolution on a Digital Freedom Strategy for EU Foreign Policy.⁶³ Elements of this strategy undoubtedly influenced the drafting of the 2014 Guidelines and are reflected in areas of the EU's external engagement discussed in the following sections.

However, despite the fact that the work of the European Parliament has been able to shape and influence the EU policies related to issues of internet freedom, its role faces limitations – particularly in the case of policy areas such as export controls for surveillance technologies, which are sensitive policy areas for member states. Despite the fact that the EU has competence to make and shape policies to promote and protect internet freedom in many different policy domains, the complex policy-making processes which require the consensus of a number of actors increase the risk

⁶³ European Parliament, "Resolution of 11 December 2012 on a Digital Freedom Strategy in EU Foreign Policy (2012/2094(INI))", *Official Journal of the European Union*, C 434/21, 23 December 2015.

of policy incoherence both horizontally (between EU policy areas) and vertically (between policies at member state and EU level).

The following sections will delve into the various aspects of the EU's external engagement in the promotion and protection of internet freedom. This will first entail a look at external engagement resulting from internal policies, before moving on to explore EU external policies aimed at promoting and protecting internet freedom. The subsequent section will assess the extent to which the EU is able to overcome the challenges posed by its fairly limited opportunity for shaping global internet governance.

EU external engagement based on internal policies

As a result of the EU's strategy for a Digital Single Market which was launched in 2015, there has been an increase in EU legislation related to internet freedom. For example, a 2015 regulation set the basis for the abolishment of EU roaming charges and created an EU-wide legal guarantee for net neutrality.⁶⁴ This means that internet service providers (ISPs) should treat all internet communications equally and not discriminate, for example, by giving faster or lower-cost access to certain sites.⁶⁵ This is an important part of ensuring internet freedom since it guarantees that ISPs do not gain a role in imposing limitations on content. The EU's approach to net neutrality has not been without criticism, but in a global context where the US has chosen to repeal its net neutrality laws, the EU (alongside India), has some of the world's most advanced requirements.⁶⁶

From an international perspective, perhaps the most impactful internet freedom legislation developed at EU level has been on the protection of user rights. This section will first discuss the external impact of the General Data Protection Regulation (GDPR)

⁶⁴ European Parliament and the Council of the European Union, "Regulation of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union", *Official Journal of the European Union*, L 310/1, 26 November 2015.

⁶⁵ *Ibid.*

⁶⁶ For an evaluation of the EU's net neutrality see: Epicenter.works, *The Net Neutrality Situation in the EU: Evaluation of the First Two Years of Enforcement*, 29 January 2019. See also: BBC News, "US officially repeals net neutrality", 11 June 2018; BBC News, "India adopts 'world's strongest' net neutrality norms", 12 July 2018.

and forthcoming ePrivacy Regulation before moving on to discuss the externalisation of EU internal policies in candidate countries for EU accession. This analysis will take into account the ability of the EU “by virtue of its existence, to exert influence beyond its borders”.⁶⁷ This concerns the EU’s structural power, combining understandings about the fundamental nature or identity of the Union with the (often unintended) consequences of EU policies.⁶⁸

Beyond borders: GDPR and the forthcoming ePrivacy Regulation

The EU has an accumulation of internal legal and policy *acquis* which has been introduced in order to enshrine Article 8 of the European Charter of Human Rights concerning the protection of personal data and Article 7 concerning the respect for private and family life, home and communications.⁶⁹ The 2002 ePrivacy Directive, the landmark 2014 European Court of Justice decision on the Right to be Forgotten,⁷⁰ the GDPR, which came into effect in May 2018, and the ePrivacy Regulation proposed in 2017 have all contributed significantly to the international debate on internet privacy.⁷¹ Building on the 1995 Data Protection Directive, the GDPR introduced a data governance framework which consists of common requirements pertaining to the processing of personal data of individuals inside the EU.⁷² Although also not without its criticism, the GDPR has been heralded as “one of the most ambitious attempts to regulate data collection in the 21st century”.⁷³ One of the most remarkable elements of the GDPR is its external implications – the onus to comply lies on any company which processes data of individuals within the EU, meaning that even companies based outside the EU could face repercussions for violations of the regulation.⁷⁴ The forthcoming ePrivacy Regulation, which is due to replace the 2002 ePrivacy Directive to

⁶⁷ Bretherton & Vogler, *op. cit.*, p. 24.

⁶⁸ *Ibid.*

⁶⁹ European Union, “Charter of Fundamental Rights of the European Union”, *op. cit.*

⁷⁰ The case established that citizens have the right to request information to be removed if it appears to be “inadequate, irrelevant or no longer relevant”. See: Case C-131/12, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González*, 2012.

⁷¹ K. Komaitis, “GDPR: Going Beyond Borders”, *Internet Society*, 25 May 2018.

⁷² European Parliament and the Council of the European Union, “Regulation of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 96/46/EC (General Data Protection Regulation)”, *Official Journal of the European Union*, L 119/1, 4 May 2016.

⁷³ Freedom House, *Freedom on The Net 2018*, *op. cit.*, p. 18.

⁷⁴ C.J. Hoofnagle, B. van der Sloot & F. Zuiderveen Borgesius, “The European Union general data protection regulation: what it is and what it means”, *Information & Communications Technology Law*, 2019, vol. 28, no. 1, pp. 73-74, 93.

include new privacy rules for all electronic communications, will also apply to any firm that manages online communications in the EU.⁷⁵

Despite concerns raised by digital rights activists and internet freedom advocacy groups within the EU about loopholes in the GDPR, its entry into force led to a widespread belief that the EU was setting itself up as the 'leading voice' on internet privacy globally.⁷⁶ The Regulation's objectives are "internal rather than explicitly external", yet we see a 'spill-over' of EU internal legislation whereby the EU's external interlocutors are compelled to engage with the EU as a result of its strong presence.⁷⁷

With the possibility of fines as high as 4% of global annual turnover, companies have high incentives to comply with the GDPR.⁷⁸ When faced with the decision of whether to raise their data privacy standards exclusively for users within the EU or whether to expand these standards to all users, some companies have voluntarily opted to apply the GDPR globally.⁷⁹ For global companies, including very large ones like Microsoft, alignment of privacy regulation at a global level has been hugely desirable in order to keep costs down.⁸⁰ The GDPR has also sparked a global discussion about data privacy legislation and has even managed to have an influence on legislation in other countries. Cases can be observed where states have introduced laws which closely resemble the GDPR. For example, the influence of the GDPR on Brazil's General Data Protection Law (GDPL) is unmistakable.⁸¹ Looking beyond the similarity in the name, many elements of the Brazilian GDPL closely resemble the EU's regulation.⁸² Although it has been described as a 'watered down' GDPR, a resemblance to the EU Regulation can also be seen in the case of California's Consumer Privacy Act.⁸³ A pattern of influence reaching beyond the borders of the EU has also been predicted for the EU's upcoming ePrivacy regulation, which could also apply to firms outside of Europe.⁸⁴

⁷⁵ J. Apostle, "We survived GDPR, now another EU privacy law looms", *Financial Times*, 13 June 2018.

⁷⁶ Komaitis, "GDPR: Going Beyond Borders", *op. cit.*

⁷⁷ *Ibid.*

⁷⁸ Hoofnagle, van der Sloot & Zuiderveen Borgesius, *op. cit.*, p. 93.

⁷⁹ J. Brill, "Microsoft's commitment to GDPR, privacy and putting customers in control of their own data", *Microsoft Blogs*, 21 May 2018.

⁸⁰ *Ibid.*

⁸¹ M. Baxter, "How GDPR is shaping global data protection", *GDPR Report*, 24 August 2018.

⁸² *Ibid.*

⁸³ *Ibid.*

⁸⁴ Apostle, *op. cit.*

The size and importance of the EU's internal market leads external actors to adopt standards and procedures which resemble those of the EU.⁸⁵ In the case of the EU's GDPR, and as is also expected to be the case with the forthcoming ePrivacy regulation, firms are attracted to the size and value of the EU's internet user base. Although its global share is set to decline in coming years, the EU still represents a relatively large proportion of the world's internet users: whilst accounting for only 6.6% percent of the world's population, the EU hosts over 10% of the world's internet users.⁸⁶ Over half of the EU's member states have reached an internet penetration rate of above 90%, with these users enjoying some of the highest standards of internet freedom worldwide.⁸⁷ For international companies which handle data of EU citizens, the choice to stop providing services to the EU's relatively wealthy internet users is not one that companies are prepared to make.⁸⁸ This leaves the EU with a substantial opportunity to shape global norms according to its internal data privacy regulations.

Externalisation of EU internal policy: candidate countries for EU accession

The externalisation of EU internal policy refers to the extension of EU rules beyond its borders.⁸⁹ The EU makes use of conditionality based on the eventual prospect of EU membership in order to extend its values and norms relating to internet freedom, freedom of expression and media pluralism beyond its borders to candidate countries. Freedom of expression and media pluralism requirements are covered "in their entirety" under the Copenhagen criteria which lay out the conditions to be fulfilled by candidate countries in order to qualify for EU accession.⁹⁰ Furthermore, the requirement to adopt the EU's entire *acquis communautaire* includes the EU's regulatory standards covering telecommunications networks and the associated digital rights. The EU supports the accession process by providing legal assistance and guidance in drafting legislation, by monitoring the policies of candidate countries and by providing financial support through the IPA.⁹¹

⁸⁵ *Ibid.*

⁸⁶ Internet World Stats, "Internet Usage in the European Union", n.d.

⁸⁷ All EU countries featuring in the Freedom House 2018 'Freedom on the Net' report all classed as "free" See: Freedom House, *Freedom on The Net 2018*, *op. cit.*, p. 16.

⁸⁸ Internet World Stats, *op. cit.*

⁸⁹ C. Damro, S. Gstöhl & S. Schunz, "Analytical framework: Understanding and explaining EU external engagement", in C. Damro, S. Gstöhl & S. Schunz (eds.), *The European Union's Evolving External Engagement*, Abingdon, Routledge, 2018, p. 19.

⁹⁰ Council of the European Union, "EU Human Rights Guidelines on Freedom of Expression Online and Offline", *op. cit.*, p. 12.

⁹¹ European Commission Directorate-General for Neighbourhood and Enlargement Negotiations, "Freedom of expression and media", n.d.

External policies promoting and protecting internet freedom

This section addresses the integration of new objectives into existing EU external policies (often referred to as mainstreaming), as well as the EU's attempts to develop a more advanced form of sectoral diplomacy in the promotion of internet freedom.⁹²

Bridging the digital divide: promoting internet access worldwide

The EU has been active in the promotion of digital technologies in its development policies for over 20 years.⁹³ Over the course of the last decade, around €350 million has been devoted to digital initiatives.⁹⁴ Approximately a third of these funds have been allocated through the ENI, with the rest allocated to Africa, Asia and Latin America, primarily through the Development Corporation Instrument (DCI).⁹⁵ The EU has acknowledged and addressed digital divides, taking into account the gender divide as well as the rural-urban one.⁹⁶ The strategy of mainstreaming digital technologies into development policies is exemplified within DG DEVCO's current 'Digital4Development' framework.⁹⁷ The framework, which was introduced in November 2017, includes the promotion of affordable and secure internet access as well as support in ensuring the necessary regulatory reforms.⁹⁸ Broadly this is framed as a means of contributing towards the achievement of the UN Sustainable Development Goals – for example by boosting job productivity and creation or by empowering women and girls. Additionally, the framework refers to digital technologies specifically as a means of "enhancing democratic governance and transparency".⁹⁹ In sum, by addressing the digital divide in its development policies, the EU contributes to reducing obstacles to access – thus promoting internet freedom. Consequently, the mainstreaming of digital aspects into existing approaches to development can be seen as an element of the EU's wider commitment to promoting internet freedom.

⁹² Damro, Gstöhl & Schunz, *op. cit.*, pp. 19-20.

⁹³ European Commission, "Digital4Development: mainstreaming digital technologies and services into EU Development Policy", Commission Staff Working Document (2017)157, Brussels, 2 May 2017, p. 8.

⁹⁴ *Ibid.*

⁹⁵ *Ibid.*

⁹⁶ *Ibid.*, p. 20.

⁹⁷ *Ibid.*, pp. 1-27.

⁹⁸ *Ibid.*, p. 4.

⁹⁹ *Ibid.*, p. 3.

The No Disconnect Strategy (and its mystery disappearance)

The EU's most notable attempt to move towards a more strategic foreign policy in the promotion of internet freedom came with the launch of the No Disconnect Strategy (NDS) in December 2011. Conceived by the Vice-President of the Commission responsible for the Digital Agenda, Neelie Kroes, the strategy originally came as a direct response to the disruptions to internet freedom caused during the Arab uprisings, but its scope later expanded beyond the Southern neighbourhood. The NDS intended to "support and assist human rights defenders, civil society organizations and individual citizens against arbitrary disruptions to the Internet and other electronic communication technologies" as well as against "indiscriminate surveillance in authoritarian regimes".¹⁰⁰ The strategy proposed action in four different ways:¹⁰¹ first, by developing and providing technological tools to enhance online privacy and security of people living in non-democratic regimes;¹⁰² second, by educating and raising awareness of activists about the risks involved with online communications;¹⁰³ third, by gathering high quality intelligence about the situation 'on the ground'; and finally by developing co-operation mechanisms for the stakeholders involved to promote multilateral action and build cross-regional co-operation to protect human rights.¹⁰⁴

One of the key components of the NDS, which relates to the third point of action, was the development of a 'European Capability of Situational Awareness' (ECSA) platform, intended to map out network disruptions, human rights violations and restrictions of fundamental freedoms in connection with the digital environment. The ECSA would comprise both what is happening regarding network connectivity and traffic, alterations or restrictions, and what is happening on the ground in terms of human rights, media, legal and policy developments concerning the internet.¹⁰⁵ It was envisaged that the ECSA would enhance EU decision-making capabilities with instant and reliable information.¹⁰⁶

¹⁰⁰ European Commission Directorate-General for Communications Networks, Content and Technology, "No Disconnect Strategy Workshop: European Capability for Situational Awareness (ECSA)", 2012, p. 1.

¹⁰¹ European Commission, "Digital Agenda: Karl-Theodor zu Guttenberg invited by roes to promote internet freedom globally", *op. cit.*

¹⁰² *Ibid.*

¹⁰³ *Ibid.*

¹⁰⁴ *Ibid.*

¹⁰⁵ *Ibid.*

¹⁰⁶ *Ibid.*

Despite the commitment made in the 2014 Guidelines to build upon the NDS, by 2016 it was clear that the Strategy was suffering from a lack of ownership and that the programme had failed to take off due to a lack of co-ordination between the various units involved.¹⁰⁷ Many elements of the strategy are still in place: as the following sections will demonstrate, the EU maintains a strategy of multi-stakeholder co-operation and has established policies and initiatives which provide assistance and tools to activists. However, despite the publication of a feasibility study for the ECSA in 2015, no further developments have emerged on the matter. An interview with a Commission official at DG CONNECT confirmed that the initiative appears to have been abandoned.¹⁰⁸ Interviews with officials at DG CONNECT and DG DEVCO revealed that many elements of the NDS are still in operation, but there is no now clear ownership for the strategy.¹⁰⁹

Support for EU Delegations: Media4Democracy

The EU is currently developing a programme to provide technical assistance to EU Delegations in the implementation of the EU's commitments to freedom of expression online and offline as outlined in the 2014 Guidelines. Media4Democracy, which was established in January 2017 under the EIDHR by the European Commission's DG DEVCO, received a sum of €4.36 million in order to facilitate its activities.¹¹⁰ The team has so far worked with thirteen different EU Delegations by providing training and capacity building to the Delegation staff, as well as supporting media landscape assessments and project design.¹¹¹ Although Media4Democracy supports a range of topics addressed in the 2014 Guidelines, online media and ICT (including internet governance, digital security and data protection issues) are listed amongst the priority areas. The programme is still very much in a nascent stage, and many of the participating Delegations are attempting to identify entry points into the complex digital media landscapes.¹¹²

¹⁰⁷ C. Stupp, "EU internet freedom programme endangered by Commission muddle", *EURACTIV*, 11 February 2016.

¹⁰⁸ Interview with a DG CONNECT official, via email, 25 March 2019.

¹⁰⁹ Interview with a DG CONNECT official, via video call, 25 March 2019; Interview with a DG DEVCO official, via video call, 12 April 2019.

¹¹⁰ Center for International Media Assistance, "Donor Profile: European Commission", n.d.

¹¹¹ Media4Democracy has worked with Delegations in Honduras, The Gambia, Burkina Faso, Ghana, Botswana, Zambia, Rwanda, Burundi, Tanzania, Kyrgyzstan, Sri Lanka & Maldives, Malaysia and Indonesia. See: Media4Democracy, "Where We Work", n.d.

¹¹² Interview with a DG DEVCO official, via video call, 12 April 2019.

Support for online media, journalists and civil society activists

Perhaps one of the strongest areas of EU external engagement in the promotion and protection of internet freedom is the promotion of online freedom of expression through the provision of direct support for civil society. Through various funding mechanisms and initiatives co-ordinated by DG NEAR, DG DEVCO and the EED, the EU is able to support established media outlets as well as so-called 'citizen journalists', including bloggers, social media activists and online human rights defenders.¹¹³ EU support for specifically online freedom of expression can be difficult to trace due to the fact that the EU's policies and programmes do not generally make a clear distinction between support for online and offline media. However, EU mechanisms for civil society support have been adapting over time in order to cater for the increasing relevance of online journalism and activism, as well as the growing need to support digital human rights defenders.

The EU's most important funding instrument for supporting and protecting civil society activists is the EIDHR. The EIDHR, which was granted a budget of €2,332.75 million for the period of 2014-2020 supports civil society organisations and human rights defenders based on calls for proposals.¹¹⁴ The EIDHR's commitment to supporting online freedom of expression is reflected in the fact that one of the specific objectives named in the 2018 global call for proposals was to "support civic activism and participation by leveraging digital technologies".¹¹⁵

Given that improvements in surveillance technology have increased governments' abilities to monitor and track online activists, the EU's work in supporting human rights defenders forms an important part of the EU's efforts to protect digital rights. Around 20-25% of the EIDHR implementation budget for 2014-2020 is dedicated to the support of human rights defenders.¹¹⁶ Much of the financial support is provided in small, ad hoc grants of up to €10,000 per grant for human rights defenders in need of urgent support.¹¹⁷ To complement the grant mechanism, ProtectDefenders.eu was set up in

¹¹³ Council of the EU, "EU Human Rights Guidelines on Freedom of Expression Online and Offline", *op. cit.*, p.2.

¹¹⁴ European Commission Directorate-General for International Cooperation and Development, "European Instrument for Democracy & Human Rights", n.d.

¹¹⁵ European External Action Service, "EIDHR: 2019 Global Call for Proposals", 6 November 2018.

¹¹⁶ *Ibid.*; Interview with a DG DEVCO official, via video call, 12 April 2019.

¹¹⁷ European Commission Directorate-General for International Cooperation and Development, "Human rights defenders", n.d.

2015 in order to provide a more comprehensive direct support mechanism for human rights defenders.¹¹⁸ The initiative is implemented by a consortium of twelve international organisations who provide around the clock urgent support as well as a range of medium- and longer-term measures.¹¹⁹ These measures include trainings on digital security for online activists as well as temporary relocation and support for judicial procedures.¹²⁰

Within the context of enlargement countries, online media does not form the focal point of the programme to build support for media freedom and media integrity in candidate countries for accession. However, within DG NEAR some elements of the IPA-funded initiatives include a specific focus on supporting online local and alternative media as a means of furthering diversity of media content.¹²¹ For example, an Eastern Partnership Civil Society Hackathon in Minsk in June 2018 demonstrated a pro-active approach towards the role of ICTs in empowering civil society.¹²²

The EED was established in 2013 to provide an added-value to the existing support mechanisms and enables a more flexible mechanism for democracy support than is currently offered under programmes run by the EU institutions.¹²³ The main recipients of EED support are in the European neighbourhood – Eastern Partnership countries, the Middle East and North Africa and, as of 2018, the Western Balkans.¹²⁴ In contrast to the EIDHR, the EED operates a demand-driven funding mechanism which allows civil society organisations, pro-democracy social movements or emerging individuals activists to make direct applications without open calls for grants. Sums offered by the EED can be more flexible or even much smaller than under the EIDHR, making them more manageable for small organisations or individual activists.

¹¹⁸ *Ibid.*

¹¹⁹ *Ibid.*

¹²⁰ *Ibid.*

¹²¹ European Commission Directorate-General for Neighbourhood and Enlargement Negotiations, "Guidelines for EU support to media freedom and media integrity in enlargement countries, 2014-2020", 21 February 2014, p.10.

¹²² The EU's Eastern Partnership countries are Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine. See: Eastern Partnership Civil Society Facility, "2018 EaP Civil Society Hackathon: Video and Photo Report", 4 July 2018.

¹²³ European Endowment for Democracy, "Annual Report #2018: Supporting People Striving for Democracy", 2019, pp. 3, 15.

¹²⁴ *Ibid.*, p. 10.

Almost half of the EED's initiatives in 2018 related to media, civic activism and participation.¹²⁵ Amongst these initiatives, there is a clear importance attached to support for online journalism and activism.¹²⁶ Particularly in the case of restrictive or repressive media environments, online news sources, blogs, social networks and secure messenger services have provided new public discussion fora and have offered a way to circumvent the media bias of state-sponsored television, radio or printed press.¹²⁷ The EED also has a history of providing funding for independent media organisations and attempts to contribute towards the development of more sustainable funding sources.¹²⁸ In political contexts where sponsorship and advertising can be harder to come by, the EED has been able to fill the funding gap and even provides funding support to activists and journalists working in exile. The EED has also funded more unconventional online initiatives – such as cartoonists who break political and social taboos, podcasters who revive storytelling traditions, environmental bloggers or filmmakers who engage with their audiences through satire.¹²⁹ The effect of these bottom-up efforts is a diversification of available content, which contributes in a small but valuable way to the increase of internet freedom.

Addressing issues of cybersecurity and disinformation

The EU's 2016 Global Strategy recognises that internal and external security have become "ever more intertwined".¹³⁰ The same logic can also be applied to the question of internet freedom: we see an environment in which internal concerns related to the rise of so-called 'hybrid threats' have a significant external dimension.¹³¹ The term hybrid threat is used to describe a range of 'non-conventional' threats which include cyber-attacks or disinformation campaigns.¹³² In order to combat the dangers caused by hybrid threats the EU has proposed a range of new measures spanning 22

¹²⁵ *Ibid.*, p. 15.

¹²⁶ Interviews with EED Programme Officers, via video call, 9 April 2019 & 19 April 2019.

¹²⁷ Interview with an EED Programme Officer, via video call, 19 April 2019.

¹²⁸ Interview with a DG DEVCO official, via video call, 12 April 2019; Interview with an EED Programme Officer, via video call, 9 April 2019.

¹²⁹ European Endowment for Democracy, *op. cit.*, p. 8; Interview with an EED Programme Officer, via video call, 19 April 2019.

¹³⁰ European External Action Service, "Shared Vision, Common Action: A Stronger Europe – A Global Strategy for the European Union's Foreign and Security Policy", June 2016, p. 7.

¹³¹ European External Action Service, "A Europe that Protects: Countering Hybrid Threats", *Factsheets*, 13 June 2018.

¹³² *Ibid.*

different action areas.¹³³ These include the creation of an EU Hybrid Fusion Cell to gather information and intelligence as well as strengthened cybersecurity measures through the creation of an EU Rapid Response Force under the EU's Permanent Structured Cooperation (PESCO).¹³⁴

Following the logic that EU internal and external security concerns are increasingly intertwined, it can be argued that the motive of the EU to tackle disinformation and promote a greater media diversity in its Eastern neighbourhood centres as much around internal security concerns as it does about broader concern for the state of human rights and democracy in the region. The European Council recognised the threat of Russian disinformation campaigns in March 2015 and has since developed a number of measures, including a comprehensive multi-million euro Action Plan against Disinformation in order address the issue.¹³⁵ The EU considers the threat of Russian disinformation and election interference to be a danger for both EU member states and countries in the European neighbourhood.¹³⁶

A key element of the EU's response to Russian disinformation in the Eastern neighbourhood is the East StratCom Task Force. Set up by the European External Action Service in 2015, the Task Force has three main objectives: it aims to explain and promote EU policies towards the Eastern neighbourhood, strengthen the overall media environment in the region and improve the EU's capacity to forecast, address and respond to disinformation.¹³⁷ The East StratCom Task Force is an area of clear strategic priority for the EU, with the 2018 budget of €1.1 million scaled up nearly fivefold to €5 million for 2019.¹³⁸ Until now the focus of external action against disinformation has been on the Eastern neighbourhood. However, the 'Action Plan against Disinformation' also recognises the threat posed to the Southern neighbourhood,

¹³³ European External Action Service, "A Europe that Protects: Countering Hybrid Threats", *op. cit.*

¹³⁴ *Ibid.*; European External Action Service, "New tool to address cyber threats: the EU's Rapid Response Force", 27 June 2018.

¹³⁵ European Council, "European Council meeting (19 and 20 March 2015) – Conclusions", Brussels, 20 March 2015, p. 5; European Commission, "A Europe that Protects: The EU steps up action against disinformation", *Press Release*, Brussels, 5 December 2018.

¹³⁶ European Commission, "Action Plan against Disinformation", Brussels, 12 December 2018, p. 3.

¹³⁷ N. Bentzen, "Online disinformation and the EU's response", *European Parliamentary Research Service*, February 2019.

¹³⁸ *Ibid.*

Middle East and Africa – which could imply a future expansion of the EU's external engagement in this domain.¹³⁹

Export controls for surveillance technologies

When considering the EU's promotion and protection of internet freedom in its external action, it is also important to consider the policy incoherence that arises from flaws in the EU's export controls for surveillance technologies. Given its legal and political commitments to promote and protect human rights, the EU and its member states face a responsibility to ensure that exports of surveillance technologies do not end up in the hands of governments who may use the technologies as an aid to commit abuses of fundamental rights. This responsibility became one of acute reality in 2011 when it was revealed that EU-based companies had supplied surveillance technologies which were used by governments to commit human rights violations during the Arab uprisings. It was reported that companies in Finland, Sweden, Denmark, Ireland, the United Kingdom, France, Germany and Italy had developed surveillance technologies used in Iran, Syria, Bahrain and Tunisia.¹⁴⁰ News stories with headlines implicating European companies in cases of torture created intense pressure on the EU to establish greater control over its exports of 'spyware'.¹⁴¹

Currently, the export of ICT surveillance systems is still regulated by the 2009 Dual-Use Regulation.¹⁴² It established a common set of export control rules and criteria, as well as a specific set of control measures to be introduced by exporters. The regulation also provided for a network of authorities to support the exchange of information and a consistent implementation and enforcement of controls throughout the EU. The common EU list of dual-use items is regularly updated in order to reflect the list agreed at international level by the Wassenaar Arrangement. The EU can also adopt country-specific sanctions, as was done in 2011 when the EU sanctions on Iran and Syria were updated to include surveillance technologies.¹⁴³

¹³⁹ European Commission, "Action Plan against Disinformation", *op. cit.*, p. 3.

¹⁴⁰ J. Bronowicka & B. Wagner, "Export Controls of Surveillance Technologies", *Centre for Internet and Human Rights*, 2015.

¹⁴¹ V. Silver & B. Elgin, "Torture in Bahrain Becomes Routine With Help from Nokia Siemens", *Bloomberg*, 23 August 2011.

¹⁴² Council of the European Union, "Council Regulation (EC) No 428/2009 of 5 May 2009 setting up a Community for the regime for the control of exports, transfer, brokering and transit of dual-use items", *Official Journal of the European Union*, L 132/1, 29 May 2009.

¹⁴³ Council of the European Union, "Council Decision 2011/235/CFSP of 12 April 2011 concerning restrictive measures directed against certain persons and entities in view of the situation in Iran",

Leading the Parliament's movement for reform of the EU's export regulation, Marietje Schaake submitted over one hundred amendments to the European Commission's proposed extension of the existing export regulation.¹⁴⁴ With many of her amendments taken on board, the Commission's proposal was approved with a majority of 91% by the European Parliament in January 2019, but has been blocked by a group of nine member states.¹⁴⁵ The Czech Republic, Cyprus, Estonia, Finland, Ireland, Italy and Poland have all joined a coalition led by Sweden in standing against the proposed update.¹⁴⁶ The coalition's opposition to the Commission's proposal is justified by the reasoning that tighter export control "could seriously undermine the competitiveness of the EU-based industry".¹⁴⁷ This line of argument rejects the idea of the EU following an autonomous approach, instead viewing a harmonisation of export controls on the international level – for example in the context of the Wassenaar Arrangement – as a prerequisite for further EU controls.

Diplomatic engagement at a bilateral and multilateral level

At a bilateral level, the EU has a record of using public statements and démarches to condemn threats and violations of internet freedom, in particular making calls for greater protection of journalists' rights.¹⁴⁸ The EU also regularly addresses human rights concerns relating to the digital environment in its bilateral human rights dialogues, although very little is publicly known about the specific content of the conversations.¹⁴⁹ The effectiveness of these bilateral measures is certainly questionable: without tangible leverage, the EU stands little opportunity of changing the fundamental

Official Journal of the European Union, L100/51, 14 April 2011; Council of the European Union, "Council Decision 2011/782/CFSP of 1 December 2011 concerning restrictive measures against Syria and repealing Decision 2011/273/CFSP", *Official Journal of the European Union*, L319/55, 2 December 2011.

¹⁴⁴ European Parliament Committee on International Trade, "Amendments: Setting up a Union regime for the control of exports, transfer, brokering, technical assistance and transit of dual-use items", 11 May 2017; European Commission, "Proposal for a Regulation of the European Parliament and of the Council setting up a Union regime for the control of exports, transfer, brokering, technical assistance and transit of dual-use items", 2016/0295, Brussels, 28 September 2016.

¹⁴⁵ C. Stupp, "Nine countries unite against EU export controls on surveillance software", *EURACTIV*, 8 June 2018.

¹⁴⁶ *Ibid.*

¹⁴⁷ *Ibid.*

¹⁴⁸ See for example: European External Action Service, "Local EU statement on freedom of expression in the Russian Federation", Strasbourg, 18 April 2018.

¹⁴⁹ European Parliament Directorate-General for External Policies Policy Department, "Surveillance and censorship: The impact of technologies on human rights", Brussels, April 2015, p. 25.

approach of important global players, such as China or Russia, towards issues of internet freedom. The European Parliament's Digital Freedom Strategy has argued in favour of trade and association agreements being conditional on the respect for digital freedoms.¹⁵⁰ However, as can be seen with the insertion of human rights clauses into trade agreements more generally, application tends to be inconsistent and where actions have not matched up to its rhetoric, the EU risks appearing hypocritical.¹⁵¹ Furthermore, the EU's relative decline in economic and geopolitical importance does not put the EU in a position where it can use trade conditionality as a means to coerce rising powers such as China or Russia to alter their visions of internet sovereignty.

The EU also has limited opportunity on the multilateral level for shaping the norms and visions of large and powerful digitally authoritarian states. Instead, the EU views the multilateral setting of the annual Internet Governance Forum as an opportunity to reaffirm its commitment to the multi-stakeholder model and foster cooperation between like-minded states. Emmanuel Macron's 2018 Paris Call for Trust and Security in Cyberspace (hereinafter referred to as the Paris Call) reaffirms many of the EU's existing commitments to internet freedom – including the support for an “open, secure, stable, accessible and peaceful cyberspace”, as well as restating the fact that offline rights must also be protected online.¹⁵² It also makes a plea for increased co-operation on cybersecurity and on tackling cybercrime – including an implied reference to the need to strengthen the Budapest Convention.¹⁵³ Despite receiving hundreds of signatories, including 64 states and many leading technology companies, the US, Russia, China, Israel and Iran have all refused to sign.¹⁵⁴ Whilst it essentially commits the signatories to nothing more than an intent to take future action, the Paris Call is also unlikely to result in fundamental changes without the agreement of the world's important players.

¹⁵⁰ European Parliament Committee on Foreign Affairs, “Report on a Digital Freedom Strategy in EU Foreign Policy (2012/2094 (INI))”, *op. cit.*

¹⁵¹ J.D. Saltner, “The European Union's human rights policy: Is the EU's use of the human rights clause inconsistent?”, *Global Affairs*, vol. 4, nos. 2-3, 2018, pp. 227-289.

¹⁵² France Diplomatie, Ministry for Europe and Foreign Affairs, “Paris Call for Trust and Security in Cyberspace”, *op. cit.*

¹⁵³ *Ibid.*

¹⁵⁴ France Diplomatie, Ministry for Europe and Foreign Affairs, “List of Supporters of the Paris Call for Trust and Security in Cyberspace”, n.d.

EU external engagement: an assessment

The emergence of external engagement in the promotion and protection of internet freedom, driven by internal security concerns, serves both as an opportunity and a concern for the future of the EU's approach. On the one hand, the blurred line between internal and external concerns over hybrid threats, cybersecurity and the spread of online disinformation has brought greater attention and funding to issues of internet freedom in the European neighbourhood and beyond. On the other hand, there is a risk that internal security concerns could begin to draw funding or attention away from longer-standing instruments and organisations (such as the EIDHR or EED) which have an explicit democracy and human rights focus. It is still currently unclear how exactly internet freedom-related funding will be shared out under the Multiannual Financial Framework for 2021-2027. However, the proposal for a Neighbourhood, Development and International Cooperation Instrument (NDICI), which channels external action support for a wide range of policy areas into one single instrument, has raised questions about the future of EIDHR-funded projects.¹⁵⁵

Although the EU has succeeded at ensuring the inclusion of elements of internet freedom promotion into a variety of different policy areas, its broad approach suffers from a number of limitations. For example, the EU institutions have struggled to maintain strong leadership or guidance for the promotion and protection of internet freedom. The No Disconnect Strategy was a valiant attempt at establishing a more strategic approach to internet freedom. The strategy provided leadership to shape policies for civil society support, multilateral engagement and situational awareness. Although the EU has continued to deliver considerable infrastructural and civil society support, the lack of strategic leadership following the disappearance of the NDS was to the detriment of the establishment of an ECSA. The EU's focus on situational awareness has moved on to the measurement and tracking of hybrid threats under the intelligence and information gathering services of the Hybrid Fusion Cell. Whilst the decision to channel funding into situational awareness for hybrid threats is a fully justified move, the loss of the possibility to build an ECSA to track network disruptions, human rights violations and restrictions of fundamental freedoms in connection with the digital environment could be something that the EU and its member states come to regret. As was seen in the case of the Media4Democracy project which supports

¹⁵⁵ European Commission, "EU Budget for the Future", *Factsheets*, 14 June 2018; Interview with a DG DEVCO official, via video call, 12 April 2019.

EU Delegations in delivering on the 2014 Guidelines, the number one challenge faced by the Delegations was a lack of contextual knowledge. This suggests that the revival of plans for an ECSA – possibly as an integrated function of the already established Hybrid Fusion Cell – could offer benefits for the EU's wider democracy and human rights promotion.

In addition to the lack of strategic direction, the EU's approach to the promotion of internet freedom continues to be undermined by the EU's failure to adopt and effectively implement more stringent export controls for surveillance technologies. Where the adoption of internal internet freedom-related policies are the result of intense intergovernmental and interinstitutional bargain, the European Commission and the European Parliament, who both promote progressive agendas for the external promotion of internet freedom, rely on the co-operation of the member states to adopt progressive legislation.

Similarly, EU citizens rely on EU decision-making procedures of the EU to adopt legislation which continues to protect their basic digital rights. Amidst criticism over the recent Copyright Directive and the forthcoming regulation preventing the dissemination of terrorist content online, the EU must be sure to maintain its own high standards of internet freedom in order to preserve its external image as an upholder of digital rights.¹⁵⁶

Conclusions

This paper has analysed the EU's external engagement in the promotion and protection of internet freedom, revealing that despite limitations arising from its opportunity and capability to act, the EU has managed to establish a considerable level of external engagement. Within the last ten years, the promotion and protection of internet freedom has developed into an important area of external action, with engagement extending into a broad range of policy areas, including human rights and democracy promotion, digital policy, enlargement and neighbourhood policy, international development and trade. EU external action addresses internet freedom with regard to each of the three categories of 'obstacles to access', 'limits on content'

¹⁵⁶ See: La Quadrature du Net, "Terrorist Regulation", n.d.; La Quadrature du Net, "La Quadrature du Net calls for the European Parliament to reject the Copyright Directive", 22 March 2019.

and 'violations of user rights'. However, questions of user rights and content limitations have attracted most EU attention and funding. User rights are covered under relatively robust internal policies which have developed significant external dimensions. Protection of user rights also forms the basis of support for human rights defenders delivered under the EIDHR and through the EED. The goal of combatting content limitations forms the basis of the EU's action against disinformation as well as its support for independent media and civil society activists.

Many of the obstacles faced by the EU in the promotion of digital rights and internet freedom resemble challenges faced in the promotion of human rights and democracy more generally. Global internet freedom is shaped by the geopolitical environment in which it operates. This environment is very difficult for the EU to influence, especially outside of its neighbourhood where its political leverage is weaker. As with the field of migration, where human rights concerns are being played off against internal security concerns, there is a risk that the promotion of internet freedom will suffer as a result of the redirection of funding towards the management of hybrid threats. However, the EU's new focus on combatting disinformation could provide benefits for the promotion of internet freedom. If framed correctly, new measures to increase media diversity in the European neighbourhood could result in greater internet freedom and present new opportunities for managing the intersectionality between cybersecurity and internet freedom – one that has frequently been co-opted by digitally authoritarian states as a pretence to instigate oppressive surveillance measures.

The next years will bring both challenges and opportunities for the promotion and protection of internet freedom. Whilst a continuation of rising digital authoritarianism is likely to further increase demand for EU civil society support, the EU also has new challenges to face. The Trump administration's refusal to sign the Paris Call, decision to scrap net neutrality and lack of interest in the US Internet Freedom Program has for now lost the EU an important geopolitical ally in the promotion of internet freedom.¹⁵⁷ The introduction of 5G networks – whether installed by the Chinese technology giant Huawei or not – will bring new challenges and complexities to data and communications privacy but will also provide an opportunity for the EU to confirm its

¹⁵⁷ A. Segal, "The Internet Freedom Agenda: Not Dead, but Not Exactly Thriving", *Council on Foreign Relations*, 21 May 2018.

role as a leader in the protection of digital rights. The course of the EU's next years of internet freedom promotion will be, in part, determined by the ability of the EU to establish greater coherence between its wide range of areas of engagement. By fostering a new drive for internet freedom from within DG CONNECT, the EU could gain back some of the leadership and necessary ambition that was lost upon the retirement of Neelie Kroes from her role as European Commissioner.

Bibliography

Academic articles

Bromley, Mark *et al.*, "ICT Surveillance Systems: Trade Policy and the Application of Human Security Concerns", *Strategic Trade Review*, vol. 2, no. 2, 2016, pp. 37-52.

Bronowicka, Joanna & Ben Wagner, "Export Controls of Surveillance Technologies", Centre for Internet and Human Rights, 2015, retrieved 5 May 2019, https://www.academia.edu/14962143/Export_Controls_of_Surveillance_Technologies

Diamond, Larry, "The Road to Digital Unfreedom: The Threat of Postmodern Totalitarianism", *Journal of Democracy*, vol. 30, no. 1, 2019, pp. 20-24.

Garside, Susanna, *Democracy and Digital Authoritarianism: An Assessment of the EU's External Engagement in the Promotion and Protection of Internet Freedom*, Master's thesis, Bruges, College of Europe, 2019.

Freyburg, Tina & Lisa Gabre, "Blocking the Bottleneck: Internet Shutdowns and Ownership at Election times in Sub-Saharan Africa", *International Journal of Communication*, vol. 12, 2018, pp. 3896-3916.

Hoofnagle, Chris Jay, Bart van der Sloot & Frederik Zuiderveen Borgesius, "The European Union general data protection regulation: what it is and what it means", *Information & Communications Technology Law*, 2019, vol. 28, no. 1, pp. 65-98.

Komaitis, Konstantinos, "GDPR: Going Beyond Borders", *Internet Society*, 25 May 2018, retrieved 5 May 2019, <https://www.internetsociety.org/blog/2018/05/gdpr-going-beyond-borders>.

Kostka, Genia, "China's Social Credit Systems and Public Opinion: Explaining High Levels of Approval", *New Media & Society*, vol. 21, no. 7, 2019, pp. 1565-1593.

Pellot, Brian, "Index policy paper: Is the EU heading in the right direction on digital freedom?", *Index on Censorship*, 20 June 2013, retrieved 5 May 2019, <https://www.indexoncensorship.org/2013/06/is-the-eu-heading-in-the-right-direction-on-digital-freedom>.

Qiang, Xiao, "The Road to Digital Unfreedom: President Xi's Surveillance State", *Journal of Democracy*, vol. 30, no. 1, 2019, pp. 53-67.

Saltnes, Johanne Døhlie, "The European Union's human rights policy: Is the EU's use of the human rights clause inconsistent?", *Global Affairs*, vol. 4, nos. 2-3, 2018, pp. 227-289.

Books and book chapters

Bretherton, Charlotte & John Vogler, *The European Union as a Global Actor*, Abingdon, Routledge, 2006, 2nd edn.

Damro, Chad, Sieglinde Gstöhl & Simon Schunz, "Analytical framework: Understanding and explaining EU external engagement", in Chad Damro, Sieglinde Gstöhl & Simon Schunz (eds.), *The European Union's Evolving External Engagement*, Abingdon, Routledge, 2018, pp. 15-34.

Dendaris, Laura, *The Global War for Internet Governance*, New Haven, Yale University Press, 2014.

Glen, Carol M., *Controlling Cyberspace: The Politics of Internet Governance and Regulation*, Santa Barbara, CA, Praeger, 2018.

Kurbalija, Jovan, *An Introduction to Internet Governance*, DiploFoundaiton, Msida, 7th edn., 2016.

Margetts, Helen, "The Internet and Democracy", in William Dutton (ed.), *The Oxford Handbook of Internet Studies*, Oxford, Oxford University Press, 2013, retrieved 5 May 2019, <http://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780199589074.001.0001/oxfordhb-9780199589074-e-20>.

Official documents and institution websites

Bentzen, Naja, "Online disinformation and the EU's response", European Parliamentary Research Service, February 2019, retrieved 5 May 2019, [http://www.europarl.europa.eu/RegData/etudes/ATAG/2018/620230/EPRS_ATA\(2018\)620230_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/ATAG/2018/620230/EPRS_ATA(2018)620230_EN.pdf).

Case C-131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González, 2012.

Center for International Media Assistance, "Donor Profile: European Commission", n.d., <https://www.cima.ned.org/donor-profiles/european-commission/#case-studies>.

Council of Europe Treaty Office, "Chart of signatures and ratifications of Treaty 185: Convention on Cybercrime", n.d., retrieved 5 May 2019, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=ra4nKuX3.

Council of Europe, "Convention on Cybercrime", Budapest, 23 November 2001, retrieved 5 May 2019, <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561>.

Council of Europe, "Recommendation CM/Rec(2016)5 of the Committee of Ministers to member States on Internet freedom", 13 April 2016, retrieved 5 May 2019, https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016806415fa.

Council of the European Union, "Council Decision 2011/235/CFSP of 12 April 2011 concerning restrictive measures directed against certain persons and entities in view of the situation in Iran", *Official Journal of the European Union*, L100/51, 14 April 2011.

Council of the European Union, "Council Decision 2011/782/CFSP of 1 December 2011 concerning restrictive measures against Syria and repealing Decision 2011/273/CFSP", *Official Journal of the European Union*, L319/55, 2 Dec. 2011.

Council of the European Union, "Council Regulation (EC) No 428/2009 of 5 May 2009 setting up a Community for the regime for the control of exports, transfer, brokering and transit of dual-use items", *Official Journal of the European Union*, L 132/1, 29 May 2009.

Council of the European Union, "EU Action Plan on Human Rights and Democracy", Brussels, 20 July 2015, retrieved 5 May 2019, <http://data.consilium.europa.eu/doc/document/ST-10897-2015-INIT/en/pdf>.

Council of the European Union, "EU Human Rights Guidelines on Freedom of Expression Online and Offline", Brussels, 12 May 2014, retrieved 5 May 2019, https://eeas.europa.eu/sites/eeas/files/eu_human_rights_guidelines_on_freedom_of_expression_online_and_offline_en.pdf.

Council of the European Union, "EU Strategic Framework and Action Plan on Human Rights and Democracy", Luxembourg, 25 June 2012, retrieved 5 May 2019, https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/foraff/131181.pdf.

Eastern Partnership Civil Society Facility, "2018 EaP Civil Society Hackathon: Video and Photo Report", 4 July 2018, retrieved 5 May 2019, <http://eapcivilsociety.eu/news/project-news/2018-eap-civil-society-hackathon-3.html>.

European Commission Directorate-General for Communications Networks, Content and Technology, "No Disconnect Strategy Workshop: European Capability for Situational Awareness (ECSA)", 2012, retrieved 5 May 2019, <https://ec.europa.eu/digital-single-market/en/news/no-disconnect-strategy-workshop-european-capability-situational>.

European Commission Directorate-General for International Cooperation and Development, "European Instrument for Democracy & Human Rights", n.d., retrieved 5 May 2019, https://ec.europa.eu/europeaid/how/finance/eidhr_en.htm_en.

European Commission Directorate-General for International Cooperation and Development, "Human rights defenders", n.d., retrieved 5 May 2019, https://ec.europa.eu/europeaid/sectors/human-rights-and-governance/democracy-and-human-rights/human-rights-defenders_en.

European Commission Directorate-General for Neighbourhood and Enlargement Negotiations, "Freedom of expression and media", n.d., retrieved 5 May 2019, https://ec.europa.eu/neighbourhood-enlargement/policy/policy-highlights/freedom-of-expression-and-media_en.

European Commission Directorate-General for Neighbourhood and Enlargement Negotiations, "Guidelines for EU support to media freedom and media integrity in enlargement countries, 2014-2020", 21 February 2014, retrieved 5 May 2019, https://ec.europa.eu/neighbourhood-enlargement/sites/neighbor/files/pdf/press_corner/elarg-guidelines-for-media-freedom-and-integrity_210214.pdf.

European Commission, "A Europe that Protects: The EU steps up action against disinformation", Press Release, Brussels, 5 December 2018, retrieved 5 May 2019, http://europa.eu/rapid/press-release_IP-18-6647_en.htm.

European Commission, "Action Plan against Disinformation", Brussels, 12 December 2018, retrieved 5 May 2019, https://eeas.europa.eu/sites/eeas/files/action_plan_against_disinformation.pdf.

European Commission, "Digital Agenda: Karl-Theodor zu Guttenberg invited by Kroes to promote internet freedom globally", Press Release, Brussels, 12 December, 2011, retrieved 5 May 2019, http://europa.eu/rapid/press-release_IP-11-1525_en.htm.

European Commission, "Digital4Development: mainstreaming digital technologies and services into EU Development Policy", Commission Staff Working Document (2017)157, Brussels, 2 May 2017, retrieved 5 May 2019, https://ec.europa.eu/europeaid/sites/devco/files/swd-digital4development_part1_v3.pdf.

European Commission, "EU Budget for the Future", Factsheets, 14 June 2018, retrieved 5 May 2019, https://ec.europa.eu/commission/sites/beta-political/files/budget-may2018-neighborhood-development-cooperation_en.pdf.

European Commission, "Proposal for a Regulation of the European Parliament and of the Council setting up a Union regime for the control of exports, transfer, brokering, technical assistance and transit of dual-use items", 2016/0295, Brussels, 28 September 2016, retrieved 5 May 2019, https://eur-lex.europa.eu/resource.html?uri=cellar:1b8f930e-8648-11e6-b076-01aa75ed71a1.0013.02/DOC_1&format=PDF.

European Council, "European Council meeting (19 and 20 March 2015) – Conclusions", Brussels, 20 March 2015, retrieved 5 May 2019, <https://www.eesc.europa.eu/resources/docs/european-council-conclusions-19-20-march-2015-en.pdf>.

European External Action Service, "A Europe that Protects: Countering Hybrid Threats", Factsheets, 13 June 2018, retrieved 5 May 2019, https://eeas.europa.eu/topics/economic-relations-connectivity-innovation/46393/europe-protects-countering-hybrid-threats_en.

European External Action Service, "EIDHR: 2019 Global Call for Proposals", 6 November 2018, retrieved 5 May 2019, <https://webgate.ec.europa.eu/europeaid/online-services/index.cfm?ADSSChck=1541670696881&do=publi.detPUB&searchtype=QS&orderby=upd&orderbyad=Desc&nbPublList=15&page=1&aoref=161054>.

European External Action Service, "Local EU statement on freedom of expression in the Russian Federation", Strasbourg, 18 April 2018, retrieved 5 May 2019, https://eeas.europa.eu/delegations/council-europe/43145/local-eu-statement-freedom-expression-russian-federation_en.

European External Action Service, "New tool to address cyber threats: the EU's Rapid Response Force", 27 June 2018, retrieved 5 May 2019, https://eeas.europa.eu/topics/eu-international-cyberspace-policy/47525/new-tool-address-cyber-threats-eus-rapid-response-force_en.

European Parliament and the Council of the European Union, "Regulation of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 96/46/EC (General Data Protection Regulation)", *Official Journal of the European Union*, L 119/1, 4 May 2016.

European Parliament and the Council of the European Union, "Regulation of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union", *Official Journal of the European Union*, L 310/1, 26 November 2015.

European Parliament Committee on Foreign Affairs, "Report on a Digital Freedom Strategy in EU Foreign Policy (2012/2094 (INI))", 15 November 2012, retrieved 5 May 2019, <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2012-0374+0+DOC+PDF+V0//EN>.

European Parliament Committee on International Trade, "Amendments: Setting up a Union regime for the control of exports, transfer, brokering, technical assistance and transit of dual-use items", 11 May 2017, retrieved 5 May 2019, <https://www.marietjeschaake.eu/media/uploads/posts/1494513231-Marietje%20Schaake%20Ams%20INTA%20Dual%20Use%20Proposal.pdf>

European Parliament Directorate-General for External Policies Policy Department, "Surveillance and censorship: the impact of technologies on human rights", April 2015, retrieved 5 May 2019, [http://www.europarl.europa.eu/RegData/etudes/STUD/2015/549034/EXPO_STU\(2015\)549034_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2015/549034/EXPO_STU(2015)549034_EN.pdf).

European Parliament, "Resolution of 11 December 2012 on a Digital Freedom Strategy in EU Foreign Policy (2012/2094(INI))", *Official Journal of the European Union*, C 434/21, 23 December 2015.

European Parliamentary Research Service, "Prospects for e-democracy in Europe: Study Summary", February 2018, retrieved 5 May 2019, [http://www.europarl.europa.eu/RegData/etudes/STUD/2018/603213/EPRS_STU\(2018\)603213_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2018/603213/EPRS_STU(2018)603213_EN.pdf).

European Union, "Charter of Fundamental Rights of the European Union", *Official Journal of the European Union*, C 326/02, 26 October 2012.

European Union, "Consolidated Versions of the Treaty on European Union and the Treaty on the Functioning of the European Union of 13 December 2007", *Official Journal of the European Union*, C326, 16 October 2012.

France Diplomatie, Ministry for Europe and Foreign Affairs, "List of Supporters of the Paris Call for Trust and Security in Cyberspace", n.d., retrieved 5 May 2019, <https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in>.

France Diplomatie, Ministry for Europe and Foreign Affairs, "Paris Call for Trust and Security in Cyberspace", 11 December 2018, retrieved 5 May 2019, https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf.

Freedom Online Coalition, "About Us: Members", n.d., retrieved 5 May 2019, <https://freedomonlinecoalition.com/about-us/members>.

Freedom Online Coalition, "Freedom Online: Joint Action for Free Expression on the Internet [Founding Declaration]", 15 December 2011, retrieved 5 May 2019, <https://www.freedomonlinecoalition.com/wp-content/uploads/2014/04/1-The-Hague-FOC-Founding-Declaration-with-Signatories-as-of-2013.pdf>.

Global Network Initiative, "About", n.d., retrieved 5 May 2019, <https://globalnetworkinitiative.org/#home-menu>.

Internet Governance Forum, "About the IGF", n.d., retrieved 5 May 2019, <https://www.intgovforum.org/multilingual/tags/about>.

Media4Democracy, "Where We Work", n.d., retrieved 5 May 2019, <https://media4democracy.eu/where-we-work>.

State Council of the People's Republic of China, Planning Outline for the Construction of a Social Credit System (2014-2020), trans. R. Creemers, 14 June 2014, retrieved 5 May 2019, <https://chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020>.

U.S. Department of Justice, "Report On The Investigation Into Russian Interference In the 2016 Presidential Election", Washington, D.C., vol. 1, March 2018, retrieved 5 May 2019, <https://www.justice.gov/storage/report.pdf>.

United Nations General Assembly, "The promotion, protection and enjoyment of human rights on the Internet", Resolution 32/13, 1 July 2016, retrieved 13 January 2020, <https://digitallibrary.un.org/record/845727>.

United Nations General Assembly, "Universal Declaration of Human Rights", Resolution 217 A (III), Paris, 1948.

Wassenaar Arrangement, "About Us", n.d., retrieved 5 May 2019, <https://www.wassenaar.org/about-us/#about-us>.

Interviews

Official, DG CONNECT, European Commission, Interview, via video call, 25 March 2019.

Official, DG CONNECT, European Commission, Interview, via email, 25 March 2019.

Official, DG DEVCO, European Commission, Interview via video call, 12 April 2019.

Programme Officer, European Endowment for Democracy, Interview, via video call, 19 April 2019.

Programme Officer, European Endowment for Democracy, Interview, via video call, 9 April 2019.

News articles and blogs

Apostle, Julia, "We survived GDPR, now another EU privacy law looms", *Financial Times*, 13 June 2018, retrieved 5 May 2019, <https://www.ft.com/content/8fc3ae5c-6eee-11e8-8863-a9bb262c5f53>.

Baxter, Michael, "How GDPR is shaping global data protection", *GDPR Report*, 24 August 2018, retrieved 5 May 2019, <https://gdpr.report/news/2018/08/24/how-gdpr-is-shaping-global-data-protection>.

BBC News, "Edward Snowden: Leaks that exposed US spy programme", 17 January 2014, retrieved 5 May 2019, <https://www.bbc.com/news/world-us-canada-23123964>.

BBC News, "India adopts 'world's strongest' net neutrality norms", 12 July 2018, retrieved 5 May 2019, <https://www.bbc.com/news/world-asia-india-44796436>.

BBC News, "US officially repeals net neutrality", 11 June 2018, retrieved 5 May 2019, <https://www.bbc.com/news/technology-44438812>.

Berti, Francesco, "E-Politics for 'the people'? The case studies of Rousseau and Podemos", *The Good Lobby*, 27 September 2017, retrieved 5 May 2019, <http://thegoodlobby.eu/e-politics-for-the-people>.

Bowcott, Owen, "GCHQ data collection regime violated human rights, court rules", *The Guardian*, 13 September 2018, retrieved 5 May 2019, <https://www.theguardian.com/uk-news/2018/sep/13/gchq-data-collection-violated-human-rights-strasbourg-court-rules>.

Brill, Julie, "Microsoft's commitment to GDPR, privacy and putting customers in control of their own data", *Microsoft Blogs*, 21 May 2018, retrieved 5 May 2019, <https://blogs.microsoft.com/on-the-issues/2018/05/21/microsofts-commitment-to-gdpr-privacy-and-putting-customers-in-control-of-their-own-data>.

Cadwalladr, Carole, "Cambridge Analytica a year on: 'a lesson in institutional failure'", *The Guardian*, 17 March 2019, retrieved 5 May 2019, <https://www.theguardian.com/uk-news/2019/mar/17/cambridge-analytica-year-on-lesson-in-institutional-failure-christopher-wylie>.

Cerf, Viton G., "Internet Access Is Not A Human Right", *The New York Times*, 4 January 2012, retrieved 5 May 2019, <https://www.nytimes.com/2012/01/05/opinion/internet-access-is-not-a-human-right.html>.

La Quadrature du Net, "La Quadrature du Net calls for the European Parliament to reject the Copyright Directive", 22 March 2019, retrieved 5 May 2019, <https://www.laquadrature.net/en/2019/03/22/la-quadrature-du-net-calls-for-the-european-parliament-to-reject-the-copyright-directive>.

La Quadrature du Net, "Terrorist Regulation", n.d., retrieved 5 May 2019, <https://www.laquadrature.net/en/terreg>.

Lee, Dave, "The tactics of a Russian troll farm", *BBC News*, 16 February 2018, retrieved 5 May 2019, <https://www.bbc.com/news/technology-43093390>.

O'Driscoll Aimee, "Where are VPNs legal and where are they banned?", *Comparitech*, 13 November 2017, retrieved 5 May 2019, <https://www.comparitech.com/vpn/where-are-vpns-legal-banned>.

Ratcliffe, Rebecca & Samuel Okiror, "Millions of Ugandans quit internet services as social media tax takes effect", *The Guardian*, 27 February 2019, retrieved 13 January 2020, <https://www.theguardian.com/global-development/2019/feb/27/millions-of-ugandans-quit-internet-after-introduction-of-social-media-tax-free-speech>.

Romaniuk, Scott N. & Tobias Burgers, "How China's AI Technology Exports Are Seeding Surveillance Societies Globally", *The Diplomat*, 18 October 2018, retrieved 5 May 2019, <https://thediplomat.com/2018/10/how-chinas-ai-technology-exports-are-seeding-surveillance-societies-globally>.

Segal, Adam, "The Internet Freedom Agenda: Not Dead, but Not Exactly Thriving Either", *Council on Foreign Relations*, 21 May 2018, accessed 5 May 2019, <https://www.cfr.org/blog/internet-freedom-agenda-not-dead-not-exactly-thriving-either>.

Silver, Vernon & Elgin, Ben, "Torture in Bahrain Becomes Routine With Help from Nokia Siemens", *Bloomberg*, 23 August 2011, retrieved 5 May 2019, <https://www.bloomberg.com/news/articles/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking>.

Stupp, Catherine, "EU internet freedom programme endangered by Commission muddle", *EURACTIV*, 11 February 2016, retrieved 5 May 2019, <https://www.euractiv.com/section/development-policy/news/eu-internet-freedom-programme-endangered-by-commission-muddle>.

Stupp, Catherine, "Nine countries unite against EU export controls on surveillance software", *EURACTIV*, 8 June 2018, retrieved 5 May 2019, <https://www.euractiv.com/section/cybersecurity/news/nine-countries-unite-against-eu-export-controls-on-surveillance-software>.

Reports and policy briefs

Access Now, "Internet Shutdowns in Context: Insights from the Shutdown Tracker Optimization Project (STOP)", 13 December 2018, retrieved 5 May 2019, <https://www.accessnow.org/keepiton>.

Epicenter.works, *The Net Neutrality Situation in the EU: Evaluation of the First Two Years of Enforcement*, 29 January 2019, retrieved 5 May 2019, https://epicenter.works/sites/default/files/2019_netneutrality_in_eu-epicenter.works-r1.pdf.

European Endowment for Democracy, "Annual Report #2018: Supporting People Striving for Democracy", 2019, retrieved 5 May 2019, <https://www.democracyendowment.eu/annual-report-2018>.

Freedom House, "China Country Report: Freedom on the Net 2018", 2018, retrieved 5 May 2019, <https://freedomhouse.org/report/freedom-net/2018/china>.

Freedom House, "Freedom on the Net Methodology", retrieved 5 May 2019, <https://freedomhouse.org/report/freedom-net-methodology>.

Freedom House, "Freedom on The Net 2018", Washington, D.C., 2018, retrieved 5 May 2019, <https://freedomhouse.org/report/freedom-net/freedom-net-2018>.

Internet World Stats, "Internet Usage in the European Union", n.d., retrieved 5 May 2019, <https://www.internetworldstats.com/stats9.htm>.

Sanou, Brahim, "ICT Facts and Figures 2017", International Telecommunication Union, Geneva, 2017, retrieved 5 May 2019, <https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2017.pdf>.

List of recent EU Diplomacy Papers

For the full list of papers and free download, please visit
www.coleurope.eu/EUDP

1/2018

Elise Cuny, *The EU's New Migration Partnership with Mali: Shifting towards a Risky Security-Migration-Development Nexus*

2/2018

Sara Canali, *The Thin Veil of Change: The EU's Promotion of Gender Equality in Egypt and Tunisia*

3/2018

Bram De Botselier, Sofia López Piqueres & Simon Schunz, *Addressing the 'Arctic Paradox': Environmental Policy Integration in the European Union's Emerging Arctic Policy*

4/2018

Valentin Steinhauer, *Leaving the Paris Agreement: The United States' Disengagement from the Global Climate Regime and its Impact on EU Climate Diplomacy*

5/2018

Esther Kestemont, *What Role(s) for the European Union in National Dialogues? Lessons Learned from Yemen*

6/2018

Melanie Bonnici Bennett, *The Refugee Crisis and the EU's Externalisation of Integrated Border Management to Libya and Turkey*

1/2019

Mélanie Scheidt, *The European Union versus External Disinformation Campaigns in the Midst of Information Warfare: Ready for the Battle?*

2/2019

Hugo Nunes da Silva, *United in Adversity? The Europeanisation of EU Concertation Practices in a More Divided UN Security Council*

3/2019

Laura Schiemichen, *Madam Ambassador: A Statistical Comparison of Female Ambassadors across the U.S., German, and EU Foreign Services*

4/2019

Simone Possenti, *The Trade-Climate Nexus: Assessing the European Union's Institutionalist Approach*

5/2019

Katherine Pye, *A Means to an End or an End in Itself? The EU Integrated Approach to Conflict in Mali*

6/2019

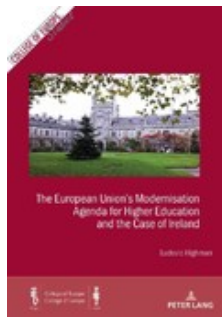
Leah McCloskey-Gholikhany, *EU Foreign Policy Identity: A Case Study on the EU's Engagement of the Islamic Republic of Iran*

7/2019

Kevin Kaiser, *EU-Morocco Negotiations on a Readmission Agreement: Obstacles to a Successful Conclusion*

1/2020

Susanna Garside, *Democracy and Digital Authoritarianism: An Assessment of the EU's External Engagement in the Promotion and Protection of Internet Freedom*



College of Europe Studies

Order online at www.peterlang.com

PIE - Peter Lang Bruxelles



- vol. 20** Highman, Ludovic, *The European Union's Modernisation Agenda for Higher Education and the Case of Ireland*, 2017 (272 p.) ISBN 978-2-8076-0616-6 pb.
- vol. 19** Bourgeois, Jacques H.J. / Marco Bronckers / Reinhard Quick (eds.), *WTO Dispute Settlement: a Check-up: Time to Take Stock*, 2017 (167 p.) ISBN 978-2-80760-377-6 pb.
- vol. 18** Schunz, Simon, *European Union Foreign Policy and the Global Climate Regime*, 2014 (371 p.), ISBN 978-2-87574-134-9 pb.
- vol. 17** Govaere, Inge / Hanf, Dominik (eds.), *Scrutinizing Internal and External Dimensions of European Law: Les dimensions internes et externes du droit européen à l'épreuve*, Liber Amicorum Paul Demaret, Vol. I and II, 2013 (880 p.), ISBN 978-2-87574-085-4 pb.
- vol. 16** Chang, Michele / Monar, Jörg (eds.), *The European Commission in the Post-Lisbon Era of Crises: Between Political Leadership and Policy Management (With a Foreword by Commission Vice President Maros Sefcovic)*, 2013 (298 p.), ISBN 978-2-87574-028-1 pb.
- vol. 15** Mahncke, Dieter / Gstöhl, Sieglinde (eds.), *European Union Diplomacy: Coherence, Unity and Effectiveness (with a Foreword by Herman Van Rompuy)*, 2012 (273 p.), ISBN 978-90-5201-7842-3 pb.
- vol. 14** Lannon, Erwan (ed.), *The European Neighbourhood Policy's Challenges / Les défis de la politique européenne de voisinage*, 2012 (491 p.), ISBN 978-90-5201-779-2 pb.
- vol. 13** Cremona, Marise / Monar, Jörg / Poli, Sara (eds.), *The External Dimension of the European Union's Area of Freedom, Security and Justice*, 2011 (434 p.), ISBN 978-90-5201-728-0 pb.
- vol. 12** Men, Jing / Balducci, Giuseppe (eds.), *Prospects and Challenges for EU-China Relations in the 21st Century: The Partnership and Cooperation Agreement*, 2010 (262 p.), ISBN 978-90-5201-641-2 pb.
- vol. 11** Monar, Jörg (ed.), *The Institutional Dimension of the European Union's Area of Freedom, Security and Justice*, 2010 (268 p.), ISBN 978-90-5201-615-3 pb.
- vol. 10** Hanf, Dominik / Malacek, Klaus / Muir Elise (dir.), *Langues et construction européenne*, 2010 (286 p.), ISBN 978-90-5201-594-1 br.
- vol. 9** Pelkmans, Jacques / Hanf, Dominik / Chang, Michele (eds.), *The EU Internal Market in Comparative Perspective: Economic, Political and Legal Analyses*, 2008 (314 p.), ISBN 978-90-5201-424-1 pb.
- vol. 8** Govaere, Inge / Ullrich, Hans (eds.), *Intellectual Property, Market Power and the Public Interest*, 2008 (315 p.), ISBN 978-90-5201-422-7 pb.
- vol. 7** Inotai, András, *The European Union and Southeastern Europe: Troubled Waters Ahead?*, 2007 (414 p.), ISBN 978-90-5201-071-7 pb.
- vol. 6** Govaere, Inge / Ullrich, Hanns (eds.), *Intellectual Property, Public Policy, and International Trade*, 2007 (232 p.), ISBN 978-90-5201-064-9 pb.