



FREEDOM ONLINE COALITION

MAY 2017

WORKING GROUP 2

Digital Development and the Rule of Law

OUTPUT DOCUMENT

REPORT OF WORKING GROUP TWO

Digital Development and the Rule of Law

OUTPUT DOCUMENT

Working Group 2 “Digital Development and the Rule of Law”

The Freedom Online Coalition Working Groups were established to explore in more detail important policy issues facing online freedom and to inform the work of the Coalition and its members. Working Group 3 seeks to explore ways to strengthen rule of law principles and good practices in a way that addresses emerging challenges, respects human rights and maximizes the impact of the Internet for social and economic development.

Co-chairs of Working Group 2

Richard Sannerholm, Folke Bernadotte Academy
Rafik Lassel Sundström, Government of Sweden

Selected Members of Working Group 2

Susan Ariel Aaronson, Renata Avila, Shagun Belwal, Lisl Brunner, Jessica Dheere, Deniz Duru Aydin, Paul Fehlinger, Patrik Hiselius, Ephraim Kenyanito, James Losey, Marilia Maciel, Andrii Paziuk, Ben Wagner.

Country Members of Working Group 2

Germany, Latvia, Moldova and United States of America

Freedom Online Coalition Support Unit

Global Partners Digital
Second Home
68-80 Hanbury Street
London
E1 5JL
+44 (0)203 818 3258

info@freedomonlinecoalition.com

CONTENTS

Executive Summary.....	07
Introduction.....	07
Summary of Findings.....	08
Recommendations.....	09
Rule of Law, Human Rights and Digital Development.....	12
Rule of Law Principles and the Global Internet.....	14
Defining Rule of Law.....	15
Challenges Facing the Application of Rule of Law Principles to the Digital Environment.....	18
Rule of Law on the Cross-Border Internet.....	18
State Measures that Undermine the Rule of Law Online: Network Disruptions and Direct Access Systems.....	19
Areas for Further Research.....	20
How Different Parts of the Online Ecosystem can Promote the Rule of Law.....	22
Resources on the Rule of Law in the Digital Environment.....	22
How to Promote Rule of Law Principles and Good Practices.....	23
Conclusion.....	27
Recommendations.....	27
ANNEX I: Members of Working Group 2.....	30
ANNEX 2: Additional Resources on the Rule of Law in the Digital Environment.....	31

01

EXECUTIVE SUMMARY

INTRODUCTION

The following report represents the culmination of the work of Working Group 2 of the Freedom Online Coalition, Digital Development and the Rule of Law. The mandate of the Working Group, which was established in spring 2015 and ends May 2017, was to identify challenges and opportunities to strengthen rule of law as a key factor in promoting digital development and respect for human rights in the digital sphere.

With this report, we aim to achieve three objectives. First, we will summarize the findings of the Working Group. Second, we will explore how different parts of the online ecosystem can promote the rule of law in the digital environment. Third, we will provide recommendations to FOC governments regarding how they can collaborate to expand the rule of law online.

The Working Group, which consists of 13 independent members of civil society, academia, and the private sector, is chaired by the Government of Sweden and the Folke Bernadotte Academy. It was established as a multistakeholder forum under the auspices of the FOC in 2015 to support implementation of the 2014 Tallinn Agenda¹, in which FOC member states committed to the following decisions:

“Dedicate ourselves, in conducting our own activities, to respect our human rights obligations, as well as the principles of the rule of law, legitimate purpose, non-arbitrariness, effective oversight, and transparency, and call upon others to do the same”

“Call upon governments worldwide to promote transparency and independent, effective domestic oversight related to electronic surveillance, use of content take-down notices, limitations or restrictions on online content or user access and other similar measures, while committing ourselves to do the same”

“Commit to preserve and strengthen the multi-stakeholder model of internet governance and increased participation in multi-stakeholder fora, such as the Internet Governance Forum”

The mission of the Working Group was to build on these commitments by exploring how to strengthen rule of law principles and good practices as a way to address emerging challenges, respect human rights and maximize the impact of the Internet for social and economic development. Members engaged in this

1. FOC Tallinn Agenda 2014

process through discussions, a blog series, and sessions at Freedom Online Conferences, the results of which are collated in this report.

In the first section of the report, we attempt to describe the interrelationship between rule of law, digital development, and human rights online. In the second section, we adopt principles of rule of law set forth by the Venice Commission and briefly discuss how they are being applied (or not) on the Internet and/or to internet governance. The third section examines three particularly current and contentious areas of rule of law online: trans-jurisdictional legal challenges, Internet disruptions, and direct-access systems, as well as highlights areas for further research. Section four presents opportunities for promoting rule of law online through greater awareness and capacity building and integration of rule-of-law principles into trade negotiations. Finally, the concluding section sets forth a set of recommendations for actions FOC members states can take to strengthen rule of law online.

We hope that this summary of our work makes a modest contribution to the broader, ongoing conversation about rule of law online, in which many stakeholders are engaged. This paper is the product of our multistakeholder Working Group, and not an official document of the Freedom Online Coalition. The report does not reflect the official views of FOC member governments (including those represented in the group), nor do they reflect new legal commitment or changes to existing legal commitments.

SUMMARY OF FINDINGS

SCOPE OF INQUIRY:

From the outset, the mandate of the Working Group implicated several distinct but interrelated areas of focus, in particular, rule of law and democracy; social and economic development and trade; Internet governance and multistakeholderism; and human rights and, by extension, human rights online. Such a multifaceted and dynamic scope of inquiry underscored the complexity of simply defining rule of law online, much less crystallizing its relationship to and effects on digital development. While there is strong agreement that strengthening rule of law online is critical to realizing the potential of digital development, identifying specific areas of intersection for further research will produce more grounded and incisive analysis and thus lead to more actionable, effective interventions.

BENEFITS:

An open, global Internet can yield enormous economic and social benefits for netizens, corporations and states and individuals, provided that it is accessible, secure, and trustworthy². Access to the Internet facilitates the exercise of human rights. It can augment civic participation and government transparency, improve access to education, allow communities to interact across borders, lead to improved medical research and healthcare, and expand the reach and power of personal expression. These social benefits can contribute to realizing economic benefits, promoting trade, innovation, and growth; these factors make the expansion of Internet access in developing countries particularly important.

2. See, One Internet. Rep. Global Commission on Internet Governance, 2016. Web. 16 May 2017. <<https://www.ourinternet.org/report>>.

CHALLENGES:

Challenges facing the open Internet have the potential to frustrate the realization of any benefits. Challenges related to the difficulty of applying the Rule of Law online include the use of the Internet for criminal and terrorist purposes, the disruption of Internet access and restriction of access to online content, surveillance by governments, the lack of interoperability of protections for personal data, and adoption of mandatory data localization laws and policies. For the digital environment to act as an enabler for development and human rights, the application of rule of law principles online is imperative. It is one of several pillars on which rests our ability to achieve sustainable technology-enabled development. The application of rule of law principles to the global Internet and Internet governance, however, is made particularly complex by several fundamental tensions, including:

- Slow progress of digital development on a global scale, revealing enduring deficits of global productivity, opportunity for the poor and the middle class, and accountable governance despite investment in technologies³.
- The rapidity with which states are developing their legal frameworks, with many laws now being applied to online spaces were originally designed for stand-alone areas such as print media or intellectual property.
- Gaps in legal texts, interpretation, and application between international and national law and regulatory regimes
- The transnational nature of the Internet as a network of networks, where infrastructure, operators, and users participating in any one network can all be located in different jurisdictions
- A need for clarity, particularly from international human rights organizations, on what the obligations of governments (and corporations) are to protect, respect, promote, and remedy violations of human rights online
- The substitution of corporate actions and policies for what have traditionally been matters for state authorities and of public and human rights law

RECOMMENDATIONS

Based on the research collated so far and the existing commitments made by the FOC, the Working Group puts forward the following recommendations.

Seek clarity from human rights bodies regarding responsibilities for human rights when other governments undermine human rights online.

Governments need clarity regarding their responsibilities for human rights when other governments undermine human rights in digital environments. The FOC should call on UN Human Rights Mechanisms to clarify the responsibilities of governments vis a vis other states. Furthermore, the UN Human Rights Mechanisms should advise governments if there is a responsibility to protect citizens in nations where rights are radically restricted or threatened, particularly where rule of law principles are not well ingrained. Additionally, if human rights mechanisms determine that governments have such an obligation, they should provide recommendations for how it can be fulfilled.

3. World Bank, World Development Report 2016: Digital Dividends, p. 2. <http://www.worldbank.org/en/publication/wdr2016>

Build on progress made on shaping global norms on issues that undermine the rule of law in the digital environment

As affirmed in the Tallinn Agenda, the Coalition should respect human rights obligations, as well as the principles of the rule of law, legitimate purpose, non-arbitrariness, effective oversight and transparency, and call upon others to do the same. The Coalition should build on its existing activities in shaping global norms through joint statements on priority issues that undermine the rule of law in the digital environment (e.g. building on Joint Statement and Best Practices on Network Disruptions or the Joint statement on Restrictive Data Localization Measures) and collectively engage with non-member governments whose actions undermine these principles.

Evaluate laws to ensure they are consistent with rule of law and human rights

In furtherance of the Coalition members' commitment to respect human rights obligations and the principles of the rule of law, each member state should evaluate any laws, state policies and private sector policies that permit measures that violate the principles of rule of law and human rights obligations. Particular areas of concern that are highlighted in the FOC underpinning documents and joint statements include state-sponsored measures that limit freedoms in a manner contrary to international human rights legal obligations, such as network disruptions, hacking of communications and establishment of direct access systems without appropriate checks and balances.

States should seek to evaluate laws and policies that enable these measures in a manner consistent with members' dedication in conducting their own activities, to respect their human rights obligations, as well as the principles of the rule of law, legitimate purpose, non-arbitrariness, effective oversight and transparency, and call on others to do the same.

Explore partnerships with expert organizations to support development of model laws

Building on the Coalition members' dedication in FOC underpinning documents to respect human rights obligations and the principles of the rule of law, and to support initiatives that promote this aim, the Coalition should explore partnerships with UNESCO and/or other expert organizations to support the development of model laws on topical policy issues such as surveillance and content restriction. These initiatives should also seek to diversify, strengthen and expand expertise by dedicating resources to build the capacity of non-English speaking partners.

Seek to hold public consultations when new laws and policies are introduced

Consistent with the FOC Founding Declaration and Tallinn Agenda, which recognise the key importance of engagement by all relevant stakeholders and underline members' commitment to work closely together in a multistakeholder process to further internet freedom, Coalition members should explore the creation of multi-stakeholder advisory bodies or groups comprised of experts who can inform the development of such laws and policies, ensure the concerns of those affected most are represented, and seek to hold public consultations at the domestic level when it introduces laws that impact the exercise of human rights online.

This would further the FOC's aim to commit to enhanced transparency of government processes and open government data initiatives as important elements in protecting human rights and fundamental freedoms.

Support and participate in multistakeholder dialogues that seek to forge solutions to cross-border challenges of internet

Consistent with the Hague Declaration and Tallinn Agenda, the Coalition and its members should support and take part in multi-stakeholder dialogues that seek to forge solutions to the conflict of laws that takes place on the global Internet. These dialogues should aim to establish predictable, transparent and accountable mechanisms for the interactions between public authorities, Internet companies and users that are as transnational as the Internet itself. They should also provide a starting point to open up global processes that remain closed for civil society. The solutions they produce have the potential to benefit developed and developing states and to deter states from taking extreme measures to control the flow of information, which are often inconsistent with rule of law principles.

For example, FOC members should work to uphold the commitments made in the recent FOC joint statement on network disruptions and encourage governments to adopt the accompanying good practices proposed by the FOC to refrain from these actions while bolstering multi-stakeholder, participatory and inclusive Internet governance, strengthening Internet infrastructure, and improving transparency.

Share best practices and provide assistance to FOC members that seek to adopt laws that may impact the exercise of human rights online

Building on the commitments outlined in the Tallinn Agenda, the Coalition should explore the establishment of a mechanism for the sharing and implementation of best practices at convenings of the FOC in order to strengthen institutional capacity of members. The Coalition could provide a unique space in which members can share information about successes and challenges in meeting member responsibilities as laid out in the Tallinn Agenda and the San José Statement. This includes the commitment to respect human rights obligations and the principles of the rule of law as outlined in the Tallinn Agenda.

The Coalition is well placed to engage in the development of resources and assistance that can be provided to states that seek to adopt laws which may impact the exercise of human rights online. If a member requests technical assistance in the drafting of any laws, Coalition members would be best placed to connect the member with resources to this end. The possibility of consultation and technical assistance might eventually be expanded to non-members of the Coalition.

Explore opportunities to convene discussions with international financial institutions and donor agencies that invest in ICT sector development

Building on the decision made in the Tallinn Agenda to support programs, initiatives and technologies that promote human rights and fundamental freedoms online, and to recommend other stakeholders to join these efforts, the Coalition is in a good position to convene discussions with international financial institutions, local governments and donor agencies that invest in key initiatives for the development of the Digital Economy. The Coalition should explore ways in which these actors can promote adherence to rule of law principles in developing states which receive financial assistance for ICT sector development.

02

RULE OF LAW, HUMAN RIGHTS & DIGITAL DEVELOPMENT

The rule of law is a principle of governance that can be traced back to the earliest forms of human civilization and represents, at its core, a will to temper or restrain the exercise of arbitrary power of the state. It is also considered an essential pillar of “sustained and inclusive economic growth, sustainable development, the eradication of poverty and hunger and the full realization of all human rights and fundamental freedoms, including the right to development...”⁴ Aspiration toward rule of law is clearly established in Agenda 2030 and the Sustainable Development Goals, in which Goal 16 is “to promote just, peaceful, and inclusive societies.”⁵

If rule of law is essential to sustainable development, it must also be so for digital development, which emphasizes harnessing digital technologies and networks to accelerate development. An open, global Internet can yield enormous economic and social benefits for states and individuals, provided that it is accessible, secure, and trustworthy. In addition to promoting rule of law, Agenda 2030 and the Sustainable Development Goals are crucially intertwined with an open, global internet, in particular regarding the goals of education; gender equality; industry, innovation and infrastructure; and peace and justice. Access to the Internet also facilitates the exercise of human rights. It can augment civic participation and government transparency, improve access to education, allow communities to interact across borders, lead to improved medical research and healthcare, and expand the reach and power of personal expression. These social benefits can contribute to realizing economic benefits, promoting trade, innovation, and growth; these factors make the expansion of Internet access in developing countries particularly important.

Over the last decade, “digital ICTs have moved from a peripheral role to a core role in our daily lives,” even in developing countries, where there are now more users from the global South and East than there are from the Global North.⁶ Despite these gains, however, there is a growing awareness that digital development hasn’t yet lived up to its promise on a global scale. According to a 2016 World Bank report, “The effect of technology on global productivity, expansion of opportunity for the poor and the middle class, and the spread of accountable governance

4. “Declaration of the High-level Meeting of the General Assembly on the Rule of Law at the National and International Levels,” A/RES/67/1, 30 November 2012 https://www.un.org/ruleoflaw/files/37839_A-RES-67-1.pdf

5. Goal 16 of the Global Goals for Sustainable Development includes as a target to “[p]romote the rule of law at the national and international levels and ensure equal access to justice for all.” Sustainable Development Goals: Goal 16: Peace, Justice, and Strong Institutions: <https://www.un.org/sustainabledevelopment/peace-justice/>

7. “Digital Development,” Report of the Secretary-General, Commission on Science and Technology for Development, Economic and Social Council, E23 February 2015.

has so far been less than expected.”⁷ Global productivity growth has slowed, labor markets are more polarized, inequality is rising, and “while the number of democracies is growing, the share of free and fair elections is falling.”⁸

The World Bank report ascribes this lack of “digital dividends” to two factors: 1) that nearly 60 percent of people are still not online, and 2) some of the perceived benefits of technologies are being offset by emerging risks. “To maximize the digital dividends requires better understanding of how technology interacts with other factors that are important for development—what the Report calls “analog components.” Among these analog components are regulations, skills, and “accountable institutions that use the internet to empower citizens.”

Challenges facing the open Internet also frustrate the realization of the promised benefits of digital development. These include use of the Internet for criminal and terrorist purposes, the disruption of Internet access and restriction of access to online content, surveillance by governments, an unregulated market for personal data, and adoption of mandatory data localization laws and policies. The magnitude of these problems has led the Global Commission for Internet Governance to warn that the Internet may become “a dangerous and broken cyberspace,” which users avoid entirely, or a driver of “uneven and unequal gains.” Alternatively, the Internet may fulfill its economic and social potential “if there is universal agreement to collectively develop a new social compact ensuring that the Internet continues on track to become more accessible, inclusive, secure and trustworthy.”⁹

In summary, for the digital environment to act as an enabler for development and human rights, the application of rule of law principles online is imperative. It is one of several pillars on which rests our ability to achieve sustainable technology-enabled development. The application of rule of law principles to the global Internet and Internet governance, however, is made particularly complex by several fundamental tensions, including:

- Slow progress of digital development on a global scale, revealing enduring deficits of global productivity, opportunity for the poor and the middle class, and accountable governance despite investment in technologies;¹⁰
- States’ application of laws originally designed for “stand-alone areas such as print media or intellectual property” to online spaces;
- Gaps in legal texts, interpretation, and application between international and national law and regulatory regimes
- The transnational nature of the Internet as a network of networks, where infrastructure, operators, and users participating in any one network can all be located in different jurisdictions
- A need for clarity, particularly from international human rights organizations,

7. World Bank, World Development Report 2016: Digital Dividends, p. 2. <http://www.worldbank.org/en/publication/wdr2016>

8. Ibid.

9. One Internet. Rep. Global Commission on Internet Governance, 2016. Web. 16 May 2017. <<https://www.ourinternet.org/report>>

10. World Bank, World Development Report 2016: Digital Dividends, p. 2. <http://www.worldbank.org/en/publication/wdr2016>

on the obligations of governments (and corporations) to protect, respect, promote, and remedy violations of human rights online; and

- The substitution of corporate actions and policies for what have traditionally been matters for state authorities and of public and human rights law

Working Group Two of the Freedom Online Coalition was formed in 2015 to consider these tensions and to explore ways to strengthen rule of law principles and good practices to address emerging issues, respect human rights and maximize the impact of the Internet for social and economic development. Through discussions, a blog series, and sessions at Freedom Online Conferences, working group members have identified current challenges and areas for future research in furtherance of this aim. The Working Group is chaired by the Government of Sweden and the Folke Bernadotte Academy and consists of 13 independent members of civil society, academia, and the private sector.¹¹ While the group has generally focused on the rule of law as it applies to states, our discussions have also touched on private sector responsibilities. We hope that this summary of our discussions makes a modest contribution to the broader, ongoing conversation about rule of law online, in which many stakeholders are engaged.

11. A list of members of Working Group Two appears in Annex One. According to the Terms of Reference of Freedom Online Working Groups, these groups “will conduct research and consultations to further public understanding of relevant Internet freedom issues. Any recommendations made through these efforts will not be binding on the Coalition or on Coalition members. Final documents will be the product of the working group itself rather than the Coalition, though they will be published on the Coalition website and made available to all Coalition members.”

03

RULE OF LAW PRINCIPLES AND THE GLOBAL INTERNET

The UN Human Rights Council has recognized that the rights that people enjoy offline must also apply online¹², and international organizations and tribunals have similarly emphasized that public international law and rule of law principles apply to the digital environment.¹³ Yet “these principles still remain largely declaratory and aspirational: there is still a deficiency in actual Internet governance arrangements that can be relied on to ensure the application of these principles in practice.”¹⁴ Thus, the application of specific rule of law principles requires clarification and adaptation to the landscape of digital development. Policymakers and companies need guidance as to how to protect and respect human rights online.

The distributed governance of the internet is an anomaly. For many years, regulation of the online dimension passed under the radar of decision-makers. At the same time, those who were engaged in developing and maintaining the technical protocols and policies that preserved the interoperability, and thus openness, of the Internet held a general view that self-governing virtual communities could resolve most problems via consensus. Over the last 10 years, however—with the advent of the participatory Web and nearly half the world’s population online—we are facing an assertion of state power online and the emergence of national Internet policy regimes that can conflict not only with international law and human rights obligations but also digital development objectives. These disjointed governance efforts pose a challenge to the application of the rule of law in a digitally connected world. The question is no longer whether the Internet can or should be governed, but rather how it should be governed: what kind of global institutions, frameworks and approaches it requires to be governed effectively.¹⁵ In order to ensure the enjoyment of human rights online – including the rights to freedom of opinion and expression, freedom of assembly and association, protection of the law against arbitrary interference with privacy, and the freedom of religion or belief – it is essential that rule of law principles form the basis for these governance mechanisms.

DEFINING RULE OF LAW:

The United Nations has defined the rule of law as “a principle of governance in which all persons, institutions and entities, public and private, including the State itself are accountable to laws that are publicly promulgated, equally enforced and independently adjudicated, and which are consistent with international human

12. Human Rights Council, The promotion, protection and enjoyment of human rights on the Internet, A/HRC/20/L.13, 29 June 2012.

13. See Annex 2 for a list of resources on this topic that have informed the work of the group.

14. The rule of law on the internet and the wider digital world, Issue Paper, Council of Europe, 2014.

15. Mueller L. Milton, Networks and States: the Global Politics of Internet Governance, Cambridge, 2010 pp. 2-3; Andrii Paziuk, WG2 Blog Internet Governance and the Rule of law .

rights norms and standards. It requires, as well, measures to ensure adherence to the principles of supremacy of law, equality before the law, accountability to the law, fairness in the application of the law, separation of powers, participation in decision-making, legal certainty, avoidance of arbitrariness and procedural and legal transparency."¹⁶ In addition to these principles, laws and their application should adhere to fundamental human rights.

Rule of law as a principle of governance means that the application of these principles should be respected whenever the state interacts with individuals and private actors, whether through legislation, regulation or other forms of exercise of power (ranging from decisions of governments to decisions by local self-governments on practical every-day matters such as licenses, property rights, and other services). This applies in both national and international interactions.¹⁷

The Venice Commission has identified some general properties of a rule of law based-system, drawing on key principles in constitutional texts, laws and regulations, including:

- Legality – government powers are authorised by law; government powers are limited by legislature and subject to independent judicial review; government powers are limited by independent audit and review; transitions of power are subject to law
- Legal certainty – laws are applied generally with equal treatment and absence of discrimination; non-retroactivity of measures applies; due process and timely proceedings in criminal, civil and administrative matters; effective enforcement of government regulations; government regulations are enforced without improper influence; government discretion is subject to law, and conforms to proportionality and necessity of legitimate aims
- Accountability - sanctions for government officials for official misconduct; the right to appeal decisions taken by government officials and agents
- Transparency - laws are clear, publicized and accessible; laws are relatively stable over time; there is a degree of public participation in decision-making and formulation of laws and policies; there is a possibility of requesting official information; the process of enacting laws is transparent; and
- Respect for fundamental rights – access to justice, the right to be heard, right to a legally competent judge, the right to an effective remedy, the presumption of innocence.¹⁸

The application of rule of law principles to Internet governance is complex. Internet governance¹⁹ is increasingly approached through arrangements negotiated by governments, the private sector, and multi-stakeholder

16. United Nations Security Council, Report of the Secretary General, The rule of law and transitional justice in conflict and post-conflict societies, S/2004/616 (23 August 2004), para. 6; United Nations General Assembly, Report of the Secretary-General, Delivering justice: programme of action to strengthen the rule of law at the national and international levels, A/66/749 (16 March 2012), para. 2.

17. The UN defines the rule of law equally important at the national level in addition to the international level. See, Report of the Secretary-General on the Rule of Law and Transitional Justice in Conflict and Post-Conflict Societies (S/2004/616), 23 August 2004.

18. See e.g. the World Justice Project's definition of the rule of law and the European Commission for Democracy through Law (Venice Commission), Report on the Rule of Law, adopted by the Venice Commission at its 106th plenary session, 11-12 March 2016.

19. The UN Working Group on Internet Governance has defined the term as "the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet." Report of the Working Group on Internet Governance, June 2005, p 4. See also, Applying the Rule of Law Online, Freedom Online Coalition WG2 Rule of Law Blog Series

collaborations. The transnational scope, the boundless scale, and the new institutions have deeply transformed national control and traditional sovereignty over communication and information policy. This has created a new digital reality where most interactions involve multiple jurisdictions at once, based upon the physical location of companies, technical operators, servers and users.

The Group's aim is to further strengthen rule of law principles and practices that protect and promote human rights online, whilst maximizing impact for social and economic development. The following sections outline some key takeaways from group members' analysis of two specific challenges in applying the rule of law online. Whilst this is not intended to be an exhaustive analysis of all the challenges inherent in applying the rule of law online, this report aims to provide an introduction on how state responses to challenges presented by the cross-border internet often result in actions that are not only inconsistent with but also actively undermine the rule of law and, consequently, its benefits for human rights and digital development.

04

CHALLENGES FACING THE APPLICATION OF RULE OF LAW PRINCIPLES TO THE DIGITAL ENVIRONMENT

RULE OF LAW ON THE CROSS-BORDER INTERNET

Rule of law principles have been developed in the context of a Westphalian notion of territorial sovereignty and the nation state, but the digital environment is inherently cross-border. The digital reality of the 21st century is that most online interactions simultaneously involve multiple jurisdictions at once — based on the locations of servers, Internet companies, users, registrars or registries — creating a huge challenge for governance and regulation.

Courts, law enforcement agencies and data protection authorities often struggle to apply existing laws in cyberspace. If Internet companies or technical operators are located on the soil of a given country, enforcing national jurisdiction can have extraterritorial impacts on Internet users in other jurisdictions. Conversely, if citizens of a country use Internet services located in foreign jurisdictions, states struggle to enforce their national laws. In response to these governance challenges, states may resort to extreme measures that actively undermine the rule of law online, such as ordering Internet shutdowns, the large-scale restriction of online content, or the localization of data, in order to assert control over the flow of information.

Traditional modes of interstate legal cooperation are ill adapted to these new cross-border digital realities, often triggering national measures to enhance digital sovereignty as a way to overcome governance challenges.²⁰ But a legal arms race — in which individual new laws are passed in an uncoordinated manner around the world — poses its own dangers. If these new laws simply apply traditional concepts of territoriality and separation of sovereignties to the digital environment, the global, open and inherently cross-border nature of the Internet could be threatened. The global community finds itself caught in the middle, as states' actions in their own self-interest result in the deterioration of the rule of law on a global scale.

All this is to the detriment of Internet users, who face legal uncertainty as to what laws apply to their everyday actions and speech online. This becomes especially apparent in situations where users seek redress or want to appeal decisions by public or private actors located in different jurisdictions. Internet companies and technical operators also face challenges: in the absence of appropriate

20. In November 2016, the first Global Internet and Jurisdiction Conference gathered stakeholders to specifically address these challenges. See Bertrand de La Chapelle and Paul Fehlinger, *Jurisdiction on the Internet: From Legal Arms Race to transnational Cooperation*, Internet & Jurisdiction Paper (2016). f

cross-border cooperation frameworks, private actors are receiving an increasing number of direct, transnational requests from public authorities from multiple jurisdictions regarding user data, content removals or domain suspensions.

STATE MEASURES THAT UNDERMINE THE RULE OF LAW ONLINE: NETWORK DISRUPTIONS AND DIRECT-ACCESS SYSTEMS

Policymakers at the domestic and international level struggle with many problems related to the intersection of domestic rules governing the internet with international law. These include practical concerns regarding the regulation of a transnational entity with a vast scale, as well as security concerns such as the use of the internet for criminal or terrorist activities or hate speech. However, some forms of government action in response to these challenges, including the normalisation of states of exception beyond the threat of imminent danger, appear patently inconsistent with the rule of law. Working Group members have carried out research on two particular network control measures that are increasingly being used by states ostensibly to mitigate security threats and to detect and prosecute cybercrime: network disruptions and the establishment of direct access systems. The Working Group concluded that in most cases, these practices are incompatible with the protection of human rights and rule of law principles, such as transparency and accountability.

NETWORK DISRUPTIONS

Internet shutdowns are a drastic means of restricting online communications. The nonprofit Access Now has defined an Internet shutdown as “an intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information.” Shutdowns can target popular platforms and messaging services or access to the mobile Internet, and they often coincide with events such as elections or protests. Access Now has documented 15 Internet shutdowns in 2015 and 56 in 2016.²¹

International human rights experts have declared²² that internet kill switches are “absolutely impermissible under international human rights law, even in times of conflict.”²³ Similarly, the Freedom Online Coalition has strongly condemned state-sponsored network disruptions aimed at preventing political opposition and civil society from exercising the right to freedom of expression and peaceful assembly, and has previously denounced restrictions and “the wholesale blocking of social media sites, to restrict individuals from exercising their human rights online.” The Coalition has further urged governments to adopt a set of good practices that encourage all governments to refrain from network disruptions that stifle exercise of the freedoms of expression, association, and peaceful assembly online, while bolstering multi-stakeholder, participatory and inclusive Internet governance, strengthening Internet infrastructure, and improving transparency.²⁴ The Coalition highlighted that in addition to governments, companies have human rights-related responsibilities and should pursue appropriate transparency in their actions that

21. Access Now, Keep it On. Campaign <<https://www.accessnow.org/keepiton/>>

22. Human Rights Council, Res 32/13 The promotion, protection and enjoyment of human rights on the Internet (June 27, 2016)

23. Joint Declaration on Freedom of Expression and Responses to Conflict Situations (May 24, 2015).

24. Freedom Online Coalition, Statement on State-Sponsored Network Disruptions and Accompanying Good practices Document (March 2017)

may affect the exercise of human rights.²⁵ It should also be noted that network shutdowns can also have a devastating effect on digital economies. A 2016 Brookings Institution report quantified the cost of 81 shutdowns over a one-year period at \$2.4 billion in GDP globally.²⁶

Working Group members have found that Internet shutdowns are more likely to happen when laws are outdated or overbroad, when laws are not transparent, and when international standards do not disallow them. They have identified at least 27 countries in which the legal framework permits the government to shut down or take over telecommunications networks, often pursuant to broad definitions of a “national emergency” or for reasons of public security. In some countries, this occurs through informal agreements between the government and communications service providers.²⁷

DIRECT ACCESS SYSTEMS

Direct access systems allow law enforcement authorities to intercept the content of communications and to obtain non-content data by means of a direct connection to the networks of telecommunications operators. The law generally requires a court or senior government official to authorize interception beforehand, and oversight mechanisms often exist. The operator, however, does not need to be contacted before interception commences – nor can it control, or even know, which authorities are conducting surveillance and to what extent. Laws often prohibit telecommunications operators from revealing that such a system is in place, which is difficult to reconcile with the principle of transparency.

Direct access regimes may also be inconsistent with the rule of law principle of accountability. In 2015, the European Court of Human Rights considered that the absence of a requirement to show an order authorizing interception to an operator or other non-governmental actor made the SORM system of direct access in Russia “particularly prone to abuse,” and it underscored “[t]he need for safeguards against arbitrariness and abuse.” The Court suggested, however, that direct access systems could be consistent with the right to privacy and the rule of law if equipment were configured to log all interceptions, and if robust oversight mechanisms were in place.²⁸

AREAS FOR FURTHER RESEARCH:

The tensions outlined here are, of course, not exhaustive. The application of the rule of law to the digital environment raises many important challenges that need addressing. Based on the Group’s work, two areas particularly rich for future inquiry have emerged: the development of a legal equivalent to the technical interoperability of the Internet, and fostering greater accountability of states and companies by increasing transparency around state-sponsored measures that can potentially undermine the rule of law.

If we want to collectively preserve the “global and interoperable nature of the Internet” in the face of the challenges posed by its trans-border nature, and uphold the rule of law online, we need predictable, transparent and accountable

25. Freedom Online Coalition, Statement on Restrictions on Access to Social Media (August 2014).

26. West, Darrell M. “Internet shutdowns costs countries \$2.4 billion last year,” Center for Technology Innovation at Brookings, October 2016. <https://www.brookings.edu/wp-content/uploads/2016/10/intenet-shutdowns-v-3.pdf>

27. Adapted from Deniz Duru Aydin, The laws that let Internet shutdowns happen, Access Now (May 25, 2016).

28. European Court of Human Rights, Zakharov v. Russia, App. No. 47143/06 (December 4, 2015).

mechanisms for the interactions between public authorities, Internet companies and users that are as transnational as the Internet itself. We have not yet developed the legal equivalent to the technical interoperability that ensures an open, global Internet. Establishing and maintaining the rule of law on the cross-border Internet demands ongoing multistakeholder cooperation that bridges the policy silos of human rights, digital economy and cybersecurity.²⁹

In addition, more work must be done to foster greater transparency and accountability by governments and ICT companies around measures that undermine the rule of law, such as direct access systems and state-sponsored hacking.³⁰ Working Group members have suggested, for instance, that governments not only make public the laws, regulations, trade agreements, and oversight mechanisms relating to direct access, but also provide companies with interception logs and allow them to disclose statistics regarding interception and access to communications data. Such increased transparency would give civil society and oversight bodies the basis to determine whether such interferences with human rights meet the tests of legality, necessity, and proportionality.³¹

29. Adapted from Paul Fehlinger, *The Rule of Law(s) on the Cross-Border Internet*, Freedom Online Coalition WG2 Rule of Law Blog Series.

30. State-sponsored interference and hacking was explicitly mentioned in the Tallinn Agenda, which calls on governments “to halt imprisonment, harassment, physical violence, censorship, hacking as well as illicit filtering, blocking and monitoring of opposition voices and other repressive measures utilised to restrict freedom of expression and organisation online in contravention of international human rights obligations.”

31. Adapted from Lisl Brunner and Patrik Hiselius, *Direct Access Systems and the Right to Privacy*, Freedom Online Coalition WG2 Rule of Law Blog Series.

05

HOW DIFFERENT PARTS OF THE ONLINE ECOSYSTEM CAN PROMOTE THE RULE OF LAW IN THE DIGITAL ENVIRONMENT

While the collective understanding of rule of law online matures, there are significant efforts underway to strengthen rule of law principles and good practices in the digital environment, including efforts by this Working Group.³² A growing body of resources—multiple charters of so-called “digital rights,”³³ or human rights online; model laws; databases and rankings of law³⁴; and, increasingly, case law³⁵—is available for states and other stakeholders that seek to draft laws or reform existing laws that impact the exercise of human rights on the Internet and facilitate social and economic development. A more complete list of these resources appears in Annex Two, and some examples are provided below.

RESOURCES ON THE RULE OF LAW IN THE DIGITAL ENVIRONMENT

Numerous experts, NGOs and intergovernmental organizations have drafted and promoted principles to define how state actions that impact the online exercise of human rights can conform to international human rights law and rule of law principles. Reports by the Office of the UN High Commissioner for Human Rights³⁶, UNESCO³⁷, the Council of Europe³⁸, and independent UN mandate holders³⁹ detail challenges and make recommendations on the protection of human rights in the digital environment. The Global Commission on Internet Governance has identified the core elements of a new social compact for the Internet.⁴⁰ Civil society organizations have prepared principles such as the **10 Internet Rights** of the multistakeholder Internet Rights and Principles Coalition and the **Necessary**

32. Please see Jessica Dheere, Pinpointing where rule of law meets human rights online, Freedom Online Coalition WG2 Rule of Law Blog Series.

33. For a compilation of dozens of such charters, see Gill, Lex, Dennis Redeker, and Urs Gasser. “Towards Digital Constitutionalism? Mapping Attempts to Craft an internet Bill of Rights.” Berkman Klein Center for Internet & Society Research Publication 2015-15. <http://nrs.harvard.edu/urn-3:HUL.InstRepos:28552582>

34. Such as the RTI Rating, “which analyses the quality of the world’s access to information laws.” <http://www.rti-rating.org/>

35. For example, Columbia University’s Global Free Expression Case Law database. <https://globalfreedomofexpression.columbia.edu/cases/>

36. The right to privacy in the digital age, A/HRC/27/37 (2014).

37. See UNESCO Series on Internet Freedom.

38. See, e.g., Guide on Human Rights for Internet Users. <<https://rm.coe.int/168008c37f>>

39. See, e.g., A/HRC/17/27 (2011); A/HRC/23/40 (2013). See also, I/A C.H.R., ‘Freedom of Expression and the Internet’, OEA/Ser.L/V/II.CIDH/RELE/INF 11/13 (December 31, 2013).

40. Global Commission on Internet Governance, One Internet (2016).

and Proportionate Principles. Organizations have created catalogues of laws that impact the exercise of human rights in the digital environment⁴¹, as well as examples of the applications of these laws.⁴²

Multiple resources also addresses the responsibility of private ICT companies to both respect the rights of users of digital communications technologies and to embed rule of law principles into their governance. These include the UN Guiding Principles on Business and Human Rights and reports by independent UN mandate holders⁴³, Working Group Three of the Freedom Online Coalition⁴⁴, and civil society organizations.⁴⁵

HOW TO PROMOTE RULE OF LAW PRINCIPLES AND GOOD PRACTICES

While this Working Group affirms the need to apply rule of law principles to the digital environment, the precise means and methods of doing so remain a work in progress. This uncertainty is owed, in part, to the fact that 1) no state can exercise control over the internet as a whole and 2) governments have not yet found consensus with regard to their responsibilities to protect human rights online. For instance, in June 2016, the UN Human Rights Council affirmed for the third time that “the same rights that people have offline must also be protected online” in a resolution supported by more than 70 states and 80 civil society organizations. Yet a vocal minority of states, including some democracies, voiced opposition to the resolution.

Jorgensen and Marzouki state that “in practice the modalities of the online realm provide significant challenges to human rights protection, many of which remain largely unexplored.”⁴⁶ They also question the status of new “digital rights,” such as the right to access the internet and the right to be forgotten and their relationship to “democratic participation.” Rule of law principles, when applied in the digital environment, yield similar allenges, as outlined above. As a result, while the introduction of legislation and policies are important means of securing the rule of law, on their own they are not enough. Without investment in resources to ensure those responsible for upholding the rule of law have the capacity and capability to evaluate the challenges and dilemmas that arise in the space between the principle of rule of law online and its practice, the rule of law will remain weak.

Several avenues are available to states committed to strengthening rule of law principles and good practices for the digital environment. They include resources dedicated to courts, independent audit commissions and national human rights

41. See, e.g., RedLatAm, published in 2013 by Derechos Digitales; the Arab Digital Rights Datasets (ADRD), developed by Social Media Exchange; the Internet Legislation Atlas, developed by Hivos and Article 19; and the Telecommunications Industry Dialogue’s resource of 44 countries’ legal frameworks regarding state powers to restrict the content of communications and to access communications content and data.

42. See, e.g., Global Voices’ Threatened Voices project; Columbia University’s Global Freedom of Expression Legal Database; Council of Europe, Filtering, Blocking, and Takedown of Illegal Content on the Internet (2016); Internet & Jurisdiction’s Retrospect Database. For more information, see Jessica Dheere, Pinpointing where rule of law meets human rights online, Freedom Online Coalition WG2 Rule of Law Blog Series.

43. A/HRC/32/38 (2016).

44. Freedom Online Coalition Working Group Three Report: Privacy and Transparency Online (November 2015).

45. See, e.g., Council of Europe and FGV Direito Rio, Terms of Service and Human Rights (2016).

46. Rikke Frank Jorgensen, Maryem Marzouki. “Reshaping the Human Rights Legacy in the Online Environment, L’Observateur des Nation Unies, Association française pour les Nations Unies, 2015, Droits de l’homme 2.0 : quelle protection à l’ère du numérique ?, 38, pp. 17-33. <http://afnuaix.free.fr>

agencies; instituting legislative drafting processes that include public consultation; supporting existing multistakeholder processes and inviting non-government stakeholders into a wider range of discussions; highlighting rule of law principles in bilateral and multilateral interactions with other states, including the negotiation of trade agreements; and seeking capacity building opportunities to develop a deeper understanding of the implications of state actions for rule of law in the digital environment.

When adopting domestic laws that impact the exercise of human rights on the Internet, the rule of law requires that the process be inclusive and transparent, enabling the participation of all stakeholders, including the private sector, civil society, academia and the technical community.⁴⁷ Several good examples of public consultation around such laws exist among Freedom Online Coalition members.⁴⁸ Laws and policies should be assessed by all stakeholders at their drafting stage and evaluated periodically and continuously with regard to the impact that their implementation may have on the core values of stability, interoperability, security and resilience of the Internet ecosystem⁴⁹, as well as on the exercise of human rights online.

Multistakeholder processes to facilitate policymaking for the digital environment can be ad hoc or take place as more formal, ongoing initiatives. Examples of the latter include the Internet Governance Forum, the Internet & Jurisdiction Policy Network, and the Global Network Initiative. In order for these processes to be effective and consistent with rule of law principles, the initiatives themselves should be based on a set of rules, such as the Code of good practice on information, participation and transparency in internet governance. These rules must be based on democratic traditions, such as pluralism and accountability, to prevent any single stakeholder group from dominating the decision-making process.⁵⁰ Furthermore, steps to affirm the legitimacy and accountability of non-governmental stakeholders have been addressed through the creation of the Internet Governance Caucus at the World Summit on the Information Society (WSIS) in 2003⁵¹ and the Civil Society Coordination Group (CSCG)⁵².

The range of ongoing multistakeholder processes, however, should not distract from the fact that many spaces where Internet governance agendas are set, critical information is shared, and decisions are made remain beyond the reach of civil society. For example, key security fora, such as the global and bilateral trade and security negotiations, whose outcomes can have a permanent impact on the openness of the Internet, are off-limits to civil society, severely limiting its ability to influence such processes and advocate in the public interest.

47. Para 1.4, Recommendation CM/Rec(2016)5 of the Committee of Ministers to member States on Internet freedom (Adopted by the Committee of Ministers on 13 April 2016 at the 1253rd meeting of the Ministers' Deputies), available at: <http://merlin.obs.coe.int/redirect.php?id=18001>. See also, Wolfgang Kleinwächter, Editorial, 2011, p. 7 in Internet policy making, Mind No 2, Berlin : Internet and Society Co: laboratory, 2011; NETmundial Multistakeholder Statement, 2014.

48. See, e.g., Australian Government, Department of Communications and the Arts, Have Your Say: Guidelines for the lawful disruption of access to online services.

49. Para 11, Internet Governance Principles, NETmundial Multistakeholder Statement, Ibid. 4.

50. Samantha Dickinson, A Journey Can be More Important than the Destination: Reflecting on the CSTD WGEC, WSIS Forum 2016, 2-6 May 2016, ITU, Geneva, available at: https://www.itu.int/net4/wsis/forum/2016/Content/AgendaFiles/document/c47c777d-7fdf-47ab-bb30-d9100bc90e48/SamanthaDickinson_

51. WSIS Civil Society Internet Governance Caucus, September 12, 2004. Contribution to the Working Group on Internet Governance (WGIG), first open consultation 20-21 September, 2004, Geneva, available at: www.wgig.org/docs/csigg-caucus.doc

52. <http://internetgov-cs.org/procedures#A>. For more information, see Andrii Paziuk, Internet Governance and the Rule of Law, Freedom Online Coalition WG2 Rule of Law Blog Series.

Governments and intergovernmental organizations can seek to promote rule of law principles in the digital environment in their bilateral and multilateral relationships with other states. The members of the OECD and the members of APEC have adopted such principles. However, some governments have agreed to binding and disputable language in trade agreements. For example, in October 2015, twelve countries — including the United States, Australia, Canada, and Mexico — found common ground on binding language in the Trans-Pacific Partnership (TPP) which states that “each party shall allow the cross-border transfer of information by electronic means.” TPP signatories plan to put this language into effect, although the US will no longer participate. Under the agreement, data localization is prohibited and the free flow of information is a default. Signatories must allow such flows unless they determine they must restrict such flows for reasons of public morals, national security, privacy, or social stability. Because this language is binding and disputable, theoretically, one party could use the agreement to challenge censorship or filtering in other parties.⁵³

Trade agreements have their limitations, however. Such agreements regulate the behavior of states, not of individuals or firms, and they are generally negotiated in secret by governments, with no direct involvement from the public, and interoperability and universal standards – central to traditional Internet policy development – are not typically priorities in their design.⁵⁴ Hence, these venues are not likely to win the support of many internet stakeholders committed to multistakeholder governance.

In the future, trade agreements could help officials as they try to develop shared rules for the local and global Internet. The inclusion of binding language on cross-border information flows offers a good starting point for enabling rule of law, but it isn't sufficient for promoting the open Internet. In negotiating new agreements, policymakers should include language related to the regulatory context in which the Internet functions (such as interoperability, free expression, fair use, and due process). With such additions, officials will be better positioned to argue that trade agreements are appropriate avenues for mediating tensions between national law and cross-border flows of information.⁵⁵

States can also encourage donor, development and international financial institutions to promote rule of law principles in their ICT sector development projects in order to better ensure that the benefits of technology are genuine for the people they impact. These organizations could evaluate the risks and impacts to human rights and the rule of law in a partner country prior to financing ICT sector projects and throughout these projects' life-cycles, assessing the legal framework. Donor and development organizations might also provide training and technical capacity-building aimed at making the domestic legal framework consistent with international standards and ensuring that government officials follow them.⁵⁶

For their part, international organizations can continue to facilitate multi-stakeholder discussions and to develop and promote principles and good practices. They can also play an important role in investing more resources capacity-building and technical assistance aimed at strengthening the rule of law in the digital

53. Aaronson, Digital Trade Imbalance, <https://www.cigionline.org/publications/digital-trade-imbalance-and-its-implications-internet-governance>

54. Susan Ariel Aaronson, The Digital Trade Imbalance and Its Implications for Internet Governance, GCIG Paper No. 25. 3 February 2016

55. Adapted from Susan Ariel Aaronson, Are trade agreements an appropriate venue for promoting the Rule of Law online? Freedom Online Coalition WG2 Blog Series.

56. See, Milka Pietikainen, Rights and ICT Sector Development at the Stockholm Internet Forum (November 4, 2015).

environment, particularly among courts, independent audit commissions, national human rights agencies, etc. For example, UNESCO has undertaken a project to reinforce Latin American judicial operators' capacities and knowledge on the rights to freedom of expression, access to public information and other correlated rights through online and in-person training.⁵⁷

Finally, while rule of law is essential to healthy digital development, we recognize that laws alone are not enough. As signals or signposts, they are important, but without the supporting institutional architecture and independent actors to guarantee due process and accountability, rule of law risks becoming "distorted so as to be equivalent to 'rule by law', or 'rule by the law', or even 'law by rules,'"⁵⁸ a conception by which "law is more easily conceived as an instrument of power than as a value to be respected."⁵⁹ With this in mind, stakeholders developing global Internet policy should be wary of over-emphasising law as a mechanism for regulating Internet governance to avoid catalyzing the proliferation in rule-by-law states of legislation that purports to follow the lead of other countries but does not aim, in its text or its application, to preserve an open Internet or respect or protect human rights. Rule-by-law states should beware that such an approach to legislation will have a significant negative impact on digital development, since digital technologies "amplify the impact of good (and bad) policies, so any failure to reform means falling farther behind those who do reform."⁶⁰

57. See, UNESCO, Promoting freedom of expression and access to public information in Latin America (June 30, 2016).

58. Cite Venice Commission, Report on the Rule of Law, 2011, p 4-5.

59. Ibid, p. 8.

60. World Bank, World Development Report 2016: Digital Dividends, p. 4. <http://www.worldbank.org/en/publication/wdr2016>.

06

CONCLUSION

There is a wealth of authority to aid states that seek to apply rule of law principles to their actions that impact the online exercise of human rights, in terms of both the substance of laws and the processes that should be undertaken when adopting them. All stakeholders can play a role in promoting the adoption of these principles in developing states: when civil society organizations, experts, and intergovernmental organizations work in concert to promote rule of law principles – for example, by including them in model laws and trade agreements and by raising them in bilateral and multilateral discussions – developing states are more likely to embrace them.

To support the Freedom Online Coalition in its implementation of the 2014 Tallinn Agenda,⁶¹ we take this opportunity to offer recommendations to Coalition members on how to strengthen rule of law principles and good practices in the digital environment in a way that maximizes the impact of digital technologies for social and economic development.

RECOMMENDATIONS FOR FREEDOM ONLINE COALITION GOVERNMENTS

Seek clarity from human rights bodies regarding responsibilities for human rights when other governments undermine human rights online.

Governments need clarity regarding their responsibilities for human rights when other governments undermine human rights in digital environments. The FOC should call on UN Human Rights Mechanisms to clarify the responsibilities of governments vis a vis other states. Furthermore, the UN Human Rights Mechanisms should advise governments if there is a responsibility to protect citizens in nations where rights are radically restricted or threatened, particularly where rule of law principles are not well ingrained. Additionally, if human rights mechanisms determine that governments have such an obligation, they should provide recommendations for how it can be fulfilled.

Build on progress made on shaping global norms on issues that undermine the rule of law in the digital environment

As affirmed in the Tallinn Agenda, the Coalition should respect human rights obligations, as well as the principles of the rule of law, legitimate purpose, non-

61. Ibid, p.4

arbitrariness, effective oversight and transparency, and call upon others to do the same. The Coalition should build on its existing activities in shaping global norms through joint statements on priority issues that undermine the rule of law in the digital environment (e.g. building on Joint Statement and Best Practices on Network Disruptions or the Joint statement on Restrictive Data Localization Measures) and collectively engage with non-member governments whose actions undermine these principles.

Evaluate laws to ensure they are consistent with rule of law and human rights

In furtherance of the Coalition members' commitment to respect human rights obligations and the principles of the rule of law, each member state should evaluate any laws, state policies and private sector policies that permit measures that violate the principles of rule of law and human rights obligations. Particular areas of concern that are highlighted in the FOC underpinning documents and joint statements include state-sponsored measures that limit freedoms in a manner contrary to international human rights legal obligations, such as network disruptions, hacking of communications and establishment of direct access systems without appropriate checks and balances.

States should seek to evaluate laws and policies that enable these measures in a manner consistent with members' dedication in conducting their own activities, to respect their human rights obligations, as well as the principles of the rule of law, legitimate purpose, non-arbitrariness, effective oversight and transparency, and call on others to do the same.

Explore partnerships with expert organizations to support development of model laws

Building on the Coalition members' dedication in FOC underpinning documents to respect human rights obligations and the principles of the rule of law, and to support initiatives that promote this aim, the Coalition should explore partnerships with UNESCO and/or other expert organizations to support the development of model laws on topical policy issues such as surveillance and content restriction. These initiatives should also seek to diversify, strengthen and expand expertise by dedicating resources to build the capacity of non-English speaking partners.

Seek to hold public consultations when new laws and policies are introduced

Consistent with the FOC Founding Declaration and Tallinn Agenda, which recognise the key importance of engagement by all relevant stakeholders and underline members' commitment to work closely together in a multistakeholder process to further internet freedom, Coalition members should explore the creation of multi-stakeholder advisory bodies or groups comprised of experts who can inform the development of such laws and policies, ensure the concerns of those affected most are represented, and seek to hold public consultations at the domestic level when it introduces laws that impact the exercise of human rights online.

This would further the FOC's aim to commit to enhanced transparency of government processes and open government data initiatives as important elements in protecting human rights and fundamental freedoms.

Support and participate in multistakeholder dialogues that seek to forge solutions to cross-border challenges of internet

Consistent with the Hague Declaration and Tallinn Agenda, the Coalition and its members should support and take part in multi-stakeholder dialogues that seek

to forge solutions to the conflict of laws that takes place on the global Internet. These dialogues should aim to establish predictable, transparent and accountable mechanisms for the interactions between public authorities, Internet companies and users that are as transnational as the Internet itself. They should also provide a starting point to open up global processes that remain closed for civil society. The solutions they produce have the potential to benefit developed and developing states and to deter states from taking extreme measures to control the flow of information, which are often inconsistent with rule of law principles.

For example, FOC members should work to uphold the commitments made in the recent FOC joint statement on network disruptions and encourage governments to adopt the accompanying good practices proposed by the FOC to refrain from these actions while bolstering multi-stakeholder, participatory and inclusive Internet governance, strengthening Internet infrastructure, and improving transparency.

Share best practices and provide assistance to FOC members that seek to adopt laws that may impact the exercise of human rights online

Building on the commitments outlined in the Tallinn Agenda, the Coalition should explore the establishment of a mechanism for the sharing and implementation of best practices at convenings of the FOC in order to strengthen institutional capacity of members. The Coalition could provide a unique space in which members can share information about successes and challenges in meeting member responsibilities as laid out in the Tallinn Agenda and the San José Statement. This includes the commitment to respect human rights obligations and the principles of the rule of law as outlined in the Tallinn Agenda.

The Coalition is well placed to engage in the development of resources and assistance that can be provided to states that seek to adopt laws which may impact the exercise of human rights online. If a member requests technical assistance in the drafting of any laws, Coalition members would be best placed to connect the member with resources to this end. The possibility of consultation and technical assistance might eventually be expanded to non-members of the Coalition.

Explore opportunities to convene discussions with international financial institutions and donor agencies that invest in ICT sector development

Building on the decision made in the Tallinn Agenda to support programs, initiatives and technologies that promote human rights and fundamental freedoms online, and to recommend other stakeholders to join these efforts, the Coalition is in a good position to convene discussions with international financial institutions, local governments and donor agencies that invest in key initiatives for the development of the Digital Economy. The Coalition should explore ways in which these actors can promote adherence to rule of law principles in developing states which receive financial assistance for ICT sector development.

Annex One

MEMBERS OF WORKING GROUP TWO

Co-Chairs

Rafik Lassel Sundström
Dominique GorskaFolke
Richard Sannerholm
Katrin Nyman-Metcalf

Ministry of Foreign Affairs, Sweden
Bernadotte Academy, Sweden
Folke Bernadotte Academy, Sweden
Tallinn University of Technology, Estonia

Members

Gigi Alford
Jonah Hill
Peter Stentzler
Alise Zalite
Corina Calugaru
Susan Ariel Aaronson
Renata Avila
Shagun Belwal
Lisl Brunner
Jessica Dheere
Deniz Duru Aydin
Paul Fehlinger
Patrik Hiselius
Ephraim Percy Kenyanito
James Losey
Marilia Maciel
Andrii Paziuk
Ben Wagner

Department of State, United States
Department of Commerce, United States
Ministry of Foreign Affairs, Germany
Ministry of Foreign Affairs, Latvia
Ministry of Foreign Affairs, Moldova
George Washington University, United States
Web Foundation, Guatemala
Software Freedom Law Center, India
AT&T, United States
Social Media Exchange, Lebanon
Access Now, Turkey
Internet & Jurisdiction, France
Telia Company, Sweden
Article 19, Kenya
Stockholm University, Sweden
Center for Technology & Society, Brazil
Kyiv University, Ukraine
European University Viadrina, Germany

Annex Two

ADDITIONAL RESOURCES ON THE RULE OF LAW IN THE DIGITAL ENVIRONMENT

UNITED NATIONS

UN Report of the Secretary-General S/2004/616, "Rule of Law and Transitional Justice in Conflict and Post-Conflict Societies", August 2004. <https://www.un.org/ruleoflaw/files/2004%20report.pdf>

UN Resolution A/RES/67/1 "Declaration of the High-level Meeting of the General Assembly on the Rule of Law at the National and International Levels", September 2012. http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/67/1

UN Human Rights Council A/HRC/26/L.24, "The promotion, protection and enjoyment of human rights on the Internet", June 2014. <http://daccess-dds-ny.un.org/doc/UNDOC/LTD/G14/059/67/PDF/G1405967.pdf?OpenElement>

UN, Report of the Secretary-General A/66/749 "Delivering justice: programme of action to strengthen the rule of law at the national and international levels", March 2012. http://www.un.org/en/ga/search/view_doc.asp?symbol=A/66/749

UN "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", June 2013. <http://www.mofa.go.jp/files/000016407.pdf>

UN Human Rights Council A/HRC/17/27 "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank la Rue", May 2011. http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

UN Group on the Information Society (UNGIS) on the Post-2015 Development Agenda, May 2013. <http://www.ungis.org/Portals/0/documents/JointInitiatives/UNGIS.Joint.Statement.pdf>

UN Office of the High Commissioner for Human Rights "The Right to Privacy in the Digital Age". <http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx>

UN Office of the High Commissioner for Human Rights "Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and remedy' Framework". http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

UNESCO Outcome document from the “CONNECTing the Dots: Options for Future Action” Conference, March 2015. http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/outcome_document.pdf

ORGANIZATION FOR SECURITY AND COOPERATION EUROPE

Organization for Security and Co-operation in Europe, “Initial set of OSCE confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies”, December 2013. <http://www.osce.org/pc/109168>

COUNCIL OF EUROPE

Council of Europe, Declaration of the Committee of Ministers on Internet governance principles, Council of Europe, September 2011. <https://wcd.coe.int/ViewDoc.jsp?id=1835773>

Council of Europe, Commissioner for Human Rights “Human Rights and a changing media landscape”, December 2011. <http://www.coe.int/t/commissioner/source/prems/MediaLandscape2011.pdf>

Council of Europe Internet Governance Strategy 2012-2015 <http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Internet%20Governance%20Strategy/Internet%20Governance%20Strategy%202012%20-%202015.pdf>

Council of Europe, Declaration of the Committee of Ministers on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies, June 2013. <https://wcd.coe.int/ViewDoc.jsp?id=2074317>

Council of Europe, Issue paper “The rule of law on the Internet and in the wider digital world”, December 2014. <https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=2654047&SecMode=1&DocId=2216804&Usage=2>

Council of Europe “Guide on Human Rights for Internet Users” <http://www.coe.int/en/web/internet-users-rights/guide>

VENICE COMMISSION

Report on the Rule of Law, Study No. 512/2009, Venice Commission, March 2011. [http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD\(2011\)003rev-e](http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2011)003rev-e)

Rule of Law Checklist, Study No. 711 / 2013, Venice Commission, March 2016. [http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD\(2016\)007-e](http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2016)007-e)

DECLARATIONS, PRINCIPLES AND STATEMENTS

EU Human Rights Guidelines on Freedom of Expression Online and Offline, May 2014. http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/EN/foraff/142549.pdf

Joint Declaration on Freedom of Expression and the Internet, the United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and People’s Rights (ACHPR)

Special Rapporteur on Freedom of Expression and Access to Information, June 2011. <http://www.osce.org/fom/78309?download=true>

Necessary and Proportionate: International Principles on the Application of Human Rights to Communications Surveillance, May 2014. <https://en.necessaryandproportionate.org/text>

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

Organization for Economic Co-operation and Development, Recommendation of the Council on Principles for Internet Policy-Making, December 2011 <http://acts.oecd.org/Instruments/ShowInstrumentView.aspx?InstrumentID=270> <http://www.oecd.org/internet/innovation/48289796.pdf>

World Summit on the information society, Document WSIS-03/GENEVA/DOC/4-E “Declaration of Principles: Building the Information Society- a global challenge in the new Millennium”, December 2003. <http://www.itu.int/wsis/docs/geneva/official/dop.html>

ARTICLES, REPORTS AND BOOKS

S. A. Aronson and M. Townes, “Can Trade Policy Set Information Free?” December 2012. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2189153

S. Braman, “The Emergent Global Information Policy Regime”, in S. Braman (Ed.), *The Emergent Global Information Policy Regime*, pp. 12-37, 2004. <http://courseweb.lis.illinois.edu/~katewill/spring2011-502/502%20and%20other%20readings/braman%202004%20emergent%20regime.pdf>

L. A. Bygrave, “Internet Governance by Contract”, 2015.

Center for International Governance Innovation (CIGI), “Finding Common Ground: Challenges and Opportunities in Internet Governance and Internet Related Policy”, November 2014. <https://www.ourinternet.org/#publications/finding-common-ground-challenges-and-opportunities-in-internet-governance-and-internet-related-policy>

W. H. Dutton, A. Dopatka, M. Hills, G. Law and V. Nash, “Freedom of Connection Freedom of Expression: The Changing Legal and Regulatory Ecology Shaping the Internet”, UNESCO, 2011. <http://unesdoc.unesco.org/images/0019/001915/191594e.pdf>

Internet & Jurisdiction Policy Network, Report 2015/16. <http://www.internetjurisdiction.net/uploads/pdfs/Annual-Reports/Internet-Jurisdiction-2015-16-Report.pdf>

L. DeNardis and M. Raymond, “Thinking Clearly About Multistakeholder Internet Governance”, November 2013. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2354377

J. Losey, “Towards Information Interdependence”, in W. J. Drake and M. E. Price (Ed.) *Internet Governance: The NETmundial Roadmap*, 2014. <https://www.dropbox.com/s/xs2x6lbn2j1q3n4/Towards%20Information%20Interdependence.pdf?dl=0>

M. L. Mueller, “Networks and States: The Global Politics of Internet Governance” Cambridge, 2010. http://pages.uoregon.edu/koopman/courses_readings/phil123-net/intro/mueller_networks-and-states.pdf

Bertrand de La Chapelle and Paul Fehlinger, Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation, Internet & Jurisdiction Paper (2016).

M. Raymond and G. Smith, "Reimagining the Internet: The Need for a High-level Strategic Vision for Internet Governance", CIGI Internet Governance Papers. Paper No. 1-July 2013. <https://www.cigionline.org/publications/2013/7/reimagining-internet-need-high-level-strategic-vision-internet-governance>

R. Deibert "Bounding Cyber Power: Escalation and Restraint in Global Cyberspace,"

CIGI Internet Governance Papers. Paper No. 6 – October 2013. http://www.cigionline.org/sites/default/files/no6_2.pdf

W. J. Drake, "Governing Global Electronic Networks: International Perspectives on Policy and Power", Cambridge, 2008. http://mitpress.mit.edu/sites/default/files/titles/content/9780262042512_sch_0001.pdf



Freedom Online Coalition Support Unit

GLOBAL PARTNERS DIGITAL

Second Home
68 - 80 Hanbury Street
London E1 5JL
+44 (0)203 818 3258

freedomonlinecoalition.com

