EUROPEAN PARLIAMENT

DIRECTORATE-GENERAL FOR EXTERNAL POLICIES

POLICY DEPARTMENT

Surveillance and censorship: The impact of technologies on human rights

DROI

EN

2015

DIRECTORATE-GENERAL FOR EXTERNAL POLICIES
POLICY DEPARTMENT

STUDY

Surveillance and censorship: The impact of technologies on human rights

ABSTRACT

As human lives transition online, so do human rights. The main challenge for the European Union and other actors is to transition all human rights to the digital sphere. This report argues that the human rights-based approach can be helpful in focusing discussions about security on individuals rather than states. It provides an overview of countries and companies that pose risks to human rights in the digital sphere. It lists the most relevant international laws and standards, technical standards, business guidelines, Internet principles and policy initiatives that have been crucial in transitioning the human rights regime to the digital sphere. It also analyses the impact of recent EU actions related to Internet and human rights issues. It concludes that different elements of EU strategic policy on human rights and digital policy need be better integrated and coordinated to ensure that technologies have a positive impact on human rights. The report concludes that EU should promote digital rights in national legislation of the third countries, but also in its own digital strategies.

EP/EXPO/B/DROI/FWC/2013-08/Lot8/02 EN
April 2015 - PE 549.034

This paper was requested by the European Parliament's Subcommittee on Human Rights.

English-language manuscript was completed on 16 April 2015.

Printed in Belgium.

Authors:

Ben WAGNER, Centre for Internet and Human Rights, European University Viadrina, GERMANY

Joanna BRONOWICKA, Centre for Internet and Human Rights, European University Viadrina, GERMANY

Cathleen BERGER, Centre for Internet and Human Rights, European University Viadrina, GERMANY

Thomas BEHRNDT, Centre for Internet and Human Rights, European University Viadrina, GERMANY

Official Responsible: Anete BANDONE

Editorial Assistants: Pia VANNESTE, Liina-Triin TAMBI

Feedback of all kind is welcome. Please write to the author: anete.bandone@ep.europa.eu.

To obtain copies, please send a request to: poldep-expo@ep.europa.eu

This paper will be published on the European Parliament's online database, 'Think tank'.

The content of this document is the sole responsibility of the author and any opinions expressed therein do not necessarily represent the official position of the European Parliament. It is addressed to the Members and staff of the EP for their parliamentary work. Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy.

ISBN(pdf): 978-92-823-7024-7 ISBN(paper): 978-92-823-7025-4

doi(pdf): 10.2861/035360 doi(paper): 10.2861/676232

Table of contents

Glossary and abbreviations

CBM	Confidence building measures
CoE	Council of Europe
DG CNECT	Directorate General for Communications Networks, Content and Technology
ECHR	European Convention on Human Rights
ECJ	European Court of Justice
ECSA	European Capability for Situation Awareness
ECtHR	European Court of Human Rights
EEAS	European External Action Service
ESS	European Security Strategy
FIDH	International Federation for Human Rights (*Fédération internationale des ligues des droits de l'Homme*)
FOC	Freedom Online Coalition
GAC	Government Advisory Council
GGE	United Nations Group of Governmental Experts
GSP	EU Generalised Scheme of Preferences
gTLD	Top Level Domains
HRW	Human Rights Watch
IAB	Internet Architecture Board
ICANN	Internet Corporation for Assigned Names and Numbers
ICCPR	International Covenant on Civil and Political Rights
ICT	Information and communication technology
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum
IMSI	International Mobile Subscriber Identity
ISOC	Internet Society
LGBT	Lesbian, gay, bisexual, and transgender
OSCE	Organization for Security and Co-operation in Europe
RFC	Request for comments
RSF	Reporters Without Borders
TiSA	Trade in Services Agreement
TTIP	Transatlantic Trade and Investment Partnership
UDHR	Universal Declaration of Human Rights
UNDP	United Nations Development Programme

UNHRC	United Nations Human Rights Council
UNSR	United Nations Special Rapporteurs
WSIS	World Summit on Information Society
WTO	World Trade Organization

Executive summary

As human lives transition online, so do human rights. The main challenge for the European Union and other actors is to refine the definitions of all human rights in the digital sphere.

In recent years, many governments have upgraded their capacity to use more advanced digital tools for censorship and surveillance. The second chapter provides an overview of countries and companies that violate human rights in the digital sphere. It focuses on freedom of expression and the right to privacy, but it also attempts to demonstrate a link between offensive practices and the broader set of human rights.

The third chapter is an overview of most relevant international laws and standards developed by intergovernmental bodies, such as the United Nations and the Council of Europe, that have been crucial in transitioning the existing human rights regime to the digital sphere. It also includes technical standards, business guidelines and Internet principles, often developed with the active involvement of non-state actors.

In the fourth chapter, the impact several international policy initiatives and their current potential to protect and promote digital rights are reviewed. Those include exports controls in the Wassenaar arrangement, the WSIS process, the Freedom Online Coalition, technical sovereignty measures, extraterritorial application of human rights and technical solutions, such as encryption, promoted by international policies.

The European Union can and often does play an active and leading role in adapting the existing human rights framework to technological developments. The fifth chapter evaluates the actions taken by the EU in its external policies and digital strategies related to Internet and human rights issues in recent years. It concludes that different elements of EU strategic policy on human rights and digital policy need to be better integrated and coordinated to meet their goals.

In the final sections, the report recommends actions that would allow the EU to further promote and protect human rights in the digital sphere. The EU should promote digital rights in national legislations of third countries, but also in its own digital strategies and external policies, such as trade and development cooperation. A narrative shift towards human rights would help to achieve this goal. The EU should also support transparency and accountability of governments and private sector, as well as independent research on human rights and technology.

1 Transitioning to the digital sphere: human rights and technologies

As human lives transition online, so do human rights. While human rights were developed at a time before the accelerated dynamics of digitisation, their value to protect every individual remains the same. In order to fully enjoy their safeguards, our understandings, frameworks, the roles of different actors and tools to protect and promote human rights, these need to be refined, clarified, revised and updated. This report hopes to contribute to a better understanding of human rights in the digital age.

The key word is 'transition': human rights protections need to be effectively enforced in the digital sphere. Only then, will the affirmation "the same rights that people have offline must also be protected online" be truly meaningful. Developments in information and communication technology (ICT) have not only transformed economic, political and social life, they have also altered lives of almost every single individual in the world. Whether we like it or not, our lives are all irrevocably influenced by this transition.

In many cases, technology has allowed individuals to more fully enjoy their human rights. The impact is perhaps most striking in the case of freedom of expression: technology has allowed individuals to exercise their freedom "to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print" on an unprecedented scale (Art. 19, ICCPR) by using a whole range of new forms of communication. Human beings are increasingly empowered to disseminate information in new ways, from starting a blog to a crowd-funding campaign.

Information technology has thus also changed communication patterns, allowing human beings to interact in unexpected ways. By now, some of these developments are so natural, that we take the benefits of technology for granted. Millions of migrants around the world, for instance, stay in touch with their families and send remittances back home with the help of online tools, instead of sending an old-fashioned letter. Technology also empowers individuals to express their diverse identities; it strengthens minorities and enables collective mobilisations.

Technologies are "biased but ambivalent" (Feenberg, 1999; McCarthy, 2011); they care little about how they are used or what effects they have. Yet, the consequences of those biases on human life, as well as their relation to economic, social and political processes, need to be elaborated if human rights are to be fully protected online.

In many cases, the use of technology has also exposed individuals to new risks to their human rights. The transition of these rights to the digital sphere is very visible, since freedom of expression is nowadays frequently restricted in the form of governments censoring content online. But subjective decisions by institutions and companies who design computer algorithms to process information may just as well interfere with freedom of speech. Ensuring that such algorithms are in line with human rights standards will be just one of many challenges in the coming years.

The right to privacy in the digital sphere has received a lot of attention in recent years, as evidence continues to resurface that private data can be accessed ever easier by third parties, including governments, companies or criminals. Revelations about government surveillance, in particular by Edward Snowden, and the collection of personal data by large corporations have raised the level of awareness amongst the general public and motivated many actors to work on transitioning the right to privacy in the online sphere.

However, the process of transitioning human rights online cannot just consider freedom of expression and the right to privacy. Especially if all human rights are as valid online as they are offline, they need to be analysed and transitional effects highlighted.

The right to be presumed innocent until proven guilty is challenged in the online sphere in particular by ongoing practices of mass data collection for surveillance purposes without prior suspicion (Bauman et al., 2014). It has been credibly argued that the presumption of innocence is undermined by such anti-terror legislation (Korff, 2014). When considering the 'Umbrella Revolution' in Hong Kong or the protests around Gezi Park in Turkey, the use of digital communication to organise these movements is evident. As was the reaction of the respective governments, which used blocking and Internet outages to try and stop people from gathering and coordinating their respective demonstrations. In this respect, it becomes clear that the right to peaceful assembly and association needs to be considered in the digital sphere as well. The same can be said for economic and social rights as well as freedom from discrimination. These rights are increasingly affected by the shift to the digital sphere and will be discussed in greater detail in section 2.

At the same time, in response to concerns about national security on the Internet, a strong push towards cybersecurity can be observed. As far as online fight against terrorism (Watt & Wintour, 2015), debates about the role of encryption (Yadron, 2015) or an increasing amount of 'cyber attacks' between states (Finn, 2007) are concerned, there is an increasing desire by states to provide military and security narratives of the Internet (Dunn Cavelty, 2007). With the United States declaring "cyberattacks as the biggest threat to the economy and national security of the United States" (Arce, 2015) this is a trend that is unlikely to change any time soon. These 'cybersecurity' narratives tend to have very limited human rights dimensions and primarily focus on security aspects (Cavelty, 2014).

For example, cybersecurity narratives typically focus on private sector enforcement and take place outside of established legal frameworks (Deibert, 2003; Tikk, 2010). While this may be perceived to be a swifter response to cyber-attacks, it also serves to diminish existing constitutional protections and limit the control of the state over its own cybersecurity policy.

In conclusion, the main challenge for the European Union, its member states and other states around the world is to refine the definitions of all human rights in the online context. Moreover, the existing human rights framework needs to be re-evaluated to account for possible negative impacts of technological developments. As an important international actor, and on the basis of its long-standing commitment to human rights, the European Union can and often does play an active and leading role in this process of adapting existing human rights principles to developments in technology.

Another step that the EU should take to promote human rights is to ensure that its own internal and external policies are adapted to the digital sphere. As long as the power exerted over the digital sphere is beyond the territorial jurisdiction of sovereign states, the influence of both state actors and the European Union is limited. Therefore, cooperation and network-oriented approaches are crucial to ensure adequate transition and protection of human rights to the digital sphere, notably, since policies implemented by non-state actors, such as multinational corporations or technical organisations, can also have a far-reaching impact. Equally important in this context is ensuring coherence between internal and external dimensions of EU policies, as it is hard to justify criticism of third countries when the EU or its member states are not living up to the same standards.

One of the first steps to exercise such influence is adjusting the narrative about human rights. Currently, the military notion of cybersecurity centred on the state is gaining traction in public debates (Gilmor in LaFrance, 2015). Shifting our attention to the human dimension serves to respond to the global nature of the digital sphere. The debate should not be about boundaries, it should be about individual rights.

2 Risks and dangers to human rights in the digital sphere

In many countries around the world, individuals are at risk of human rights violations related to their use of Internet and other ICTs. It is often through examples of those violations that much was learned about the applicability of human rights online.

The list of "enemies of the internet", compiled by Reporters without Borders, is one example that can be used as a starting point for analysis[1]. It includes Bahrain, Belarus, China, Cuba, Ethiopia, India, Iran, North Korea, Pakistan, Russia, Saudi Arabia, Sudan, Syria, Turkmenistan, UK, United Arab Emirates, USA, Uzbekistan and Vietnam.

This overview is focused on freedom of expression and the right to privacy, as violations to freedom of expression and privacy are among the best documented, but it also attempts to demonstrate a link between offensive practices and the broader set of human rights.

2.1 Freedom of expression

When it comes to freedom of expression, violations are often inflicted by governments. These may employ a variety of measures including targeting dissident voices, filtering and/or blocking content and even disconnecting access to technologies altogether.

Journalists, dissidents and other individuals who share their opinions online continue to face such risk in many places around the world. The danger seems to be particularly high in Syria, where the government monitors the activities of its citizens online to such an effect that a record number of journalists were killed, with many more kidnapped or imprisoned (RSF 2014). Since 2011 the Committee for the Protection of Journalists has documented 89 cases of journalists or media workers who were killed in Syria, higher than any other country in the world during this period[2]. One of the few other countries which come close to Syria in its threat to journalists and media workers' lives is Pakistan, where 81 journalists and media workers have been killed since 1992[3].

At the same time, Syria actively uses strategies of Internet censorship and network disconnection as part of large-scale military offensives. As Anita Gohdes demonstrates, Internet "blackouts occur in conjunction with significantly higher levels of state repression, most notably in areas where government forces are actively fighting violent opposition groups […] results indicate that such network blackouts constitute a part of the military's strategy to target and weaken opposition groups, where the underreporting of violence is not systematically linked to outages." As a result, "in Syria the Internet is being used as a weapon of war" (Tanriverdi, 2015).

In Iran, individuals continue to risk severe prison punishment not only for criticising the regime, but also for publishing texts related to Sufi religion or damaging "public morality". In one infamous instance, producers and dancers of the homemade YouTube video "Happy in Tehran" were given a one-year suspended sentence in prison and 91 lashes for featuring women without headscarves

[1] See: http://12mars.rsf.org/2014-en/ for further details.

[2] See: https://cpj.org/killed/mideast/syria/ for further details.

[3] See: https://cpj.org/killed/asia/pakistan/ for further details.

(Culzac, 2014)[4]. In China, intimidation and arrests of social media users intensified during President Xi Jinping's campaign against "rumours" (RSF, 2014b).

Measures to dissuade citizens from creating their own sites and blogs can also take the form of a mandatory registration of online media with public authority. In Saudi Arabia, only nationals aged at least 20, with a high school diploma and able to produce "documents testifying to good conduct" are allowed to apply for a licence to start their own blog or website (RSF, 2014a). A similar way of controlling speech and expression is used in Belarus, where it is also required that websites providing services to the public must register using the national '.by' domain and be hosted on Belarussian territory (RSF, 2014a).

Controlling the telecommunications industry is another strategy that enables repressive regimes to filter and block content online. Iran continues to use widespread filtering and blocking of social media tools, such as Facebook and Twitter. China employs, among other means, a set of technical solutions known as the Great Firewall of China to block online content passing from abroad through the country's six Internet gateway points. In Pakistan the main web regulation agency, controlled by the government and the military, is currently blocking thousands of websites based on the fight against terrorism, condemnation of blasphemy and of pornography, as well as the protection of national interests.

Another way to control content online is temporary disconnection and slowdowns. In the weeks leading up to the elections, the government of Iran has drastically slowed speeds for encrypted traffic and blocked most international connections, for instance. Similar techniques were used in Syria and Pakistan for disrupting different key political events and demonstrations.

In countries where the telecommunications industry is not as strongly controlled by the state, governments may seek to enhance their censorship capacity by introducing new legislation. In Russia, as the protests unfolded on Euromaidan in Kiev, Vladimir Putin signed a bill allowing authorities to blacklist websites reporting on the events in Ukraine and Crimea. Further restrictions of freedom of expression were introduced with a law requiring bloggers and social media users to register with the telecommunications regulator (Birnbaum, 2014).

In Turkey mandatory filtering by Internet Service Providers was originally introduced to "protect" the population from pornography, but has since expanded to expressions of dissent with the government (Wagner, 2014)[5]. Google and Facebook were pressured to remove political content during the Gezi park protests in 2013 (Epstein, 2013). Moreover, in the run up to the elections held in March 2014, Twitter and YouTube were blocked (Jenkins, 2014). Although the Turkish Constitutional Court eventually overturned the ban, new laws have been introduced that make it easier for government authorities to block websites and intercept communications (Wagner, 2014), thus interfering with freedom of expression and speech.

2.2 The right to privacy

In recent years, many governments have upgraded their surveillance capacities, which pose numerous challenges to the right to privacy. Many repressive regimes rely on sophisticated and effective software for both targeted and mass surveillance developed mainly in Europe and North

[4] View the original video here: http://youtu.be/tg5qdlxVcz8

[5] Similar Internet filtering practices can also be observed in many other countries, with the OpenNet Project providing an excellent overview on https://opennet.net

America. The distinction between targeted and mass surveillance is important, both from a legal and policy perspective. Mass surveillance focuses on collecting all information possible from the Internet, an indiscriminate practice that is likely in breach of Art. 17 ICCPR. Targeted surveillance on the other hand focuses on a specific individual, set of individuals or regions and is thus at least potentially compliant with international human rights law (La Rue, 2013).

Several European companies have been implicated in selling surveillance technology to the Syrian government, including Qosmos from France and Ultimaco from Germany (FIDH, 2014). In the conflict in Syria targeted malware has been employed frequently and extensively (K. Lab, 2014; Scott-Railton & Hardy, 2014). At the same time attacks on Syrian Internet infrastructure and surveillance are closely linked to physical attacks such as bombings, torture and military strikes. "When a network is working, it's likely that activists will be targeted and killed. When a network isn't working that's a strong indication that an area is about to be bombed" (Tanriverdi, 2015).

The Ethiopian government is one of the many that purchased a suite of surveillance technology known as FinFisher or FinSpy, produced by Gamma International with branches in the UK and Germany. Marketed exclusively to governments, FinFisher technology was used to conduct surveillance in many countries where digital rights are systematically violated including Bahrain, Pakistan, Turkey, the United Arab Emirates and Vietnam (Citzen Lab 2013). FinFisher was also used to target the communications of three Bahraini activists and an Ethiopian political refugee living in the UK leading to the filing of a criminal complaint urging investigation of unlawful surveillance in the British National Crime Agency (FIDH, 2014).

In Iran monitoring equipment was reportedly provided by Huawei Technologies and ZTE Corporation from China, as well as Ultimaco from Germany, despite international bans on such sales (FIDH, 2014).

Although Azerbaijan does not engage in systematic or widespread blocking or filtering of websites or social networks, the country has allegedly purchased intrusion technology called HackingTeam from Italy (Marczak, Guarnieri, Marquis-Boire, & Scott-Railton, 2014). Building on these, the Azerbaijani government is believed to arrest, intimidate or even sexually harass activists and journalists and in year 2014 many of them have been detained for online activity unfavourable to the current government.

There is ample evidence, too, that the Turkish government acquired Trojan Horse technology from the Italian vendor HackingTeam and from the British/German vendor FinFisher (Ctizen Lab. Morgan Marquis-Boire, Marczak, Bill Claudio Guarnieri, 2013; Marczak et al., 2014).

It appears that mega-events serve to justify massive additional expenditures in government surveillance. This was a case before the 2014 Sochi Winter Olympic Games in Russia. A similar effect was visible in Brazil that also invested heavily into security equipment including digital command centres and mass surveillance equipment before the World Cup it hosted in 2014 (Whitefield, 2014).

Of course, the surveillance equipment is not discarded afterwards. Research into sporting events shows that governments sometimes even use the opportunity to test the latest surveillance technology, which then develops into the standard for the future (Bennett, Haggerty 2012). With such a trend that links mega-sporting events to mass surveillance, far greater consideration of human rights aspects is required already during the planning phase of similar future events.

It is important to note that there are also human rights concerns related to mass surveillance in Europe and North America. Information revealed in the Snowden files indicates that the so-called 'Five Eyes' (USA, UK, Canada, Australia, New Zealand) engage in collecting and sharing information gathered by intelligence agencies that bypass domestic regulations on surveillance. The tactics and huge variety of programs employed by the Five Eyes are at least questionable under international human rights law. As the 2014 United Nations High Commissioner for Human Rights report concluded, "Mass or "bulk" surveillance programmes may thus be deemed to be arbitrary, even if they serve a legitimate aim and have been adopted on the basis of an accessible legal regime" (Pillay, 2014).

2.3 Freedom of assembly, freedom of religion, freedom from discrimination and economic and social rights

As shown in the first chapter of this study, freedom of speech and the right to privacy are not the only human rights at stake in the digital sphere. Users of technologies have also been denied other rights, such as freedom of assembly or freedom from discrimination based on ethnicity, religion, gender or sexual orientation.

In China, technology has negatively affected rights of religious and ethnic minorities, with government targeting supporters of the Falung Gong, Tibetans and Uighurs, e.g. in 2014 a prominent Uighur academic and webmaster Ilham Tohti was sentenced to life imprisonment (Bequelin, 2014).

In Sudan, Saudi Arabia, Yemen, Mauritania, Somalia, and Iran accessing content with references to homosexuality is punishable by death (LGBT Technology Partnership, 2013), infringing the rights of sexual minorities from discrimination. More broadly, user information collected into big data sets by companies can be used for profiling sexual orientation or other sensitive data raising new human rights concerns and the need to discuss corporate responsibilities.

Importantly the underlying principle that rights apply "without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status" (Art.2, UDHR) could also benefit from an analysis of transitioning effects in order to protect individuals from new forms of discrimination. As more and more information about individuals is collected, stored and processed as 'Big Data,' there is significant scope for discriminatory practices by insurance and medical providers, search engines and 'predictive policing' (Pasquale, 2015; Tufekci, 2015). As subjective decisions transition into automated systems, there is an increasing risk of discrimination that a human rights-based approach cannot ignore. Another issue is the lack of transparency of these automated algorithmic systems, which poses challenges for those who wish to understand how these systems actually function. In a similar vein, the rights of children might need to be refined to account for threats related to technological developments (Livingstone, 2014).

Finally it should also be noted that our understanding of the impact of technologies on economic, social and cultural rights is still underdeveloped. Some of them, such as the 'right to a standard of living adequate for the health and well-being [...] including […] medical care' (Art. 25 UDHR) have not been explored from this perspective of 'transition' yet. For example, an increasing amount of users use the Internet to find health-related information online. However this information is filtered and restricted in many jurisdictions for example in case of reproductive health issues (Freedman, 1999). Another particularly sensitive area is personal health information. In just one recent example revelations about mass surveillance have led to a drop in the number of Internet users searching for 'aids', 'depression' or even 'abortion' (Marthews & Tucker, 2014). Moreover digital applications of freedom of movement and the right to counsel remain insufficiently explored.

This list of the violations listed is not exhaustive, as more evidence is needed to fully assess impact of technologies on a broad set of human rights. As state and non-state actors upgrade their technological capacity, new challenges arise to human rights.

3 Legal and regulatory safeguards for human rights

In 1947, when the modern human rights regime was born, only a small part of the world's population had access to the latest technologies such as telephony or television. Today, two-thirds of the estimated 3 billion Internet users are coming from the developing world. International laws and standards have been constantly evolving to continue to adequately protect human rights, but much work still needs to be done to account for challenges related to the digital sphere.

This section is an overview of international laws and standards developed by intergovernmental bodies, such as the United Nations or the Council of Europe. It also includes technical standards, business guidelines and principles, which are more and more often developed with the active involvement of non-state actors. The task is not to provide an exhaustive list of all relevant laws and standards, but rather to point to the ones that have been crucial in transitioning the human rights regime to the digital sphere.

3.1 Laws and standards developed in the United Nations

Human rights are recognised on the international level by *The Universal Declaration of Human Rights* (UDHR)[6] adopted by the United Nations General Assembly in 1948[7]. The UDHR stresses that the rights of every individual are universal and thus, every individual is "entitled to equal protection against any discrimination" (Art. 7). Two articles, which have been considered most relevant in the context of the development of information and communication technologies, are Article 12, which protects the individual from "arbitrary interference with his privacy, family, home or correspondence", and Article 19, which guarantees "the right to freedom of opinion and expression". The latter is composed of two complimentary freedoms: "to hold opinions without interference" and "to seek, receive and impart information and ideas through any media and regardless of frontiers." As technologies evolved, the meaning of privacy of correspondence is now understood to encompass different forms of digital communications, as do 'any media' in the context of freedom of expression.

The UDHR inspired most of the legally binding human rights treaties in existence today, including the *International Covenant on Civil and Political Rights* (ICCPR) which entered into force in 1976 and is legally binding for the states that ratified it. In the ICCPR the right to privacy is repeated verbatim in Article 17, while Article 19 on freedom of opinion and expression is expanded to include possible restrictions on the basis of "rights or reputations of others" and "the protection of national security or of public order or of public health or morals". It should be noted that Article 19 introduces the tension between freedom of expression and national security, which is still very much present in debates about human rights in the digital sphere and is a constantly reoccurring theme in the current political narratives.

Beyond cybersecurity, the role of independent experts appointed by the United Nations Human Rights Council (UNHRC), who examine and report back on a country situation or specific human rights, is particularly important in developing international human rights. The UN Special Rapporteurs (UNSR) issue declarations and reports that suggest new lines of interpretation and possible amendments to the human rights regime; while these interpretations have encountered political resistance, they pave the way to transitioning human rights law.

[6] Full text available here: https://www.un.org/en/documents/udhr/index.shtml

[7] Back in 1948, eight UN member states abstained from the vote, however, none dissented.

The Rapporteur best equipped to deal directly with challenges brought about by digital technologies is the UNSR on the promotion and protection of the right to freedom of opinion and expression established in 1993. His mandate is to, inter alia, "make recommendations and providing suggestions on ways and means to better promote and protect the right to freedom of opinion and expression in all its manifestations"[8].

The assessment of digital challenges is a prominent part of the legacy of former U.N. Special Rapporteur for Freedom of Expression, Frank La Rue. He successfully integrated voices from across the globe through an extensive consultation process that informed both his 2011 *Report to the General Assembly on the right to freedom of opinion and expression exercised through the Internet* and his 2013 *Report to the Human Rights Council on the implications of States' surveillance of communications on the exercise of the human rights to privacy and to freedom of opinion and expression*[9]. Both enrich our understanding of how the Internet affects human rights and are commonly regarded as some of the key reports in this area.

As of August 2014, he was replaced by David Kaye, whose report on the legal framework governing the relationship between freedom of expression and the use of encryption to secure transactions and communications, and other technologies to transact and communicate anonymously online is expected to be presented in June 2015[10].

In 2012 the UNHRC adopted by consensus a *Resolution on the promotion, protection and enjoyment of human rights on the Internet*. The Resolution included a momentous affirmation that "the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice" (A/HRC/20/L.13)[11]. The document also recognised the global and open nature of the Internet as a driving force in accelerating progress towards development and encourages special procedures to take these issues into account within their existing mandates.

As the issue of privacy online grew in prominence in recent years, it is now expected that the HRC will adopt a resolution in its 28th session (March 2015) establishing a new Special Rapporteur on the right to privacy. This is a result the Snowden revelations starting in 2013 which increased concerns about the negative impact that surveillance and interception of communications may have on human rights. This motivated the General Assembly to adopt a *Resolution on the right to privacy in the digital age*. Not only does the Resolution call upon all States to protect the right to privacy in the context of digital communication and to put an end to violations of that right, but also "to review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection" (A/RES/68/167).

In her 2014 report on the right to privacy in the digital age, the former UN High Commissioner for Human Rights, Navi Pillay, contributed significantly by stating that while intrusive surveillance might be allowed, it is the responsibility of governments to demonstrate that "interference is both necessary and proportionate to the specific risk being addressed." As meeting this condition is impossible in the case of mass or "bulk" surveillance programmes, they "may thus be deemed to be arbitrary, even if

[8] See http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/OpinionIndex.aspx
[9] See http://ap.ohchr.org/documents/dpage_e.aspx?si=A/66/290 and http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/23/40
[10] See http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx
[11] http://ap.ohchr.org/documents/E/HRC/d_res_dec/A_HRC_20_L13.doc

they serve a legitimate aim and have been adopted on the basis of an accessible legal regime," Pillay concludes[12].

The report contributed to the revision of the *Resolution on the right to privacy in the digital age* by the third committee of the UN General Assembly in November of 2014, which was extended to include a call for all States to "establish or maintain existing independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data", as well as "to provide individuals whose right to privacy has been violated by unlawful or arbitrary surveillance with access to an effective remedy, consistent with international human rights obligations"[13].

The recommendations included in the Resolution can be considered to be new international standard on the right to privacy as applied to the digital sphere. However, political frictions surrounding negotiations of its draft text made it evident that contested issues such as the principle of proportionality, the interpretation and use of metadata or the notion of extraterritoriality demand further attention and in-depth research. The work of a new UNSR on the right to privacy could contribute to dissolving conflicts of interpretation and thus to strengthening the human rights regime in the digital age. Here, General Comment 34 of the UN Human Rights Committee on the Right to Freedom of Expression and Opinion Article 19 of the ICCPR can also be helpful. It was updated in 2011 and provides valuable additional analysis, in particular in regards to the protections of Article 19 that explicitly extend to "electronic and internet-based modes of expression"[14]. However, what is still missing is an updated General Comment on the Right to Privacy in Article 17 of the ICCPR. The current General Comment 16 stems from 1988 and although it mentions "computers, data banks and other devices"[15] it does not mention the Internet or even digital communications at all.

The UN Group of Governmental Experts (GGE) also attempts to better define norms and obligations of states in cyberspace. While this group is heavily focussed on state security and conflicts between governments, it also considers "information and communications technologies in conflicts and how international law applies to the use of information and communications technologies" as well as "norms, rules or principles of responsible behaviour of States" (A/RES/69/28). This does not imply that states act irresponsibly on the Internet, but is derived from the classical diplomatic understanding (as well as experience from disarmament efforts) that a space seemingly beyond anyone's control could be used as a weapon. Therefore the group attempts to develop common norms and "confidence building measures" (A/RES/69/28) which may help to de-escalate situations of uncertainty.

As technologies evolve, similar revisions of laws, standards and tools applied by the UN might include human rights other than freedom of expression and the right to privacy. The UN is however, not the only international forum, where important work on codifying laws, guidelines or principles applicable to the digital sphere has been done by actors responsible for protection of human rights.

[12] Full text available here: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf
[13] Full text available here: http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/69/L.26/Rev.1
[14] Full text available here: http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf
[15] See http://www.refworld.org/docid/453883f922.html for further details.

3.2 Laws and standards developed in other international bodies[16]

In recent years, important work in transitioning human rights online has been done not only at intergovernmental level, but also in multistakeholder processes initiated by technical organisations, private actors and civil society. As the Internet intersects political, social and economic spheres of human activity, conversations about updating laws, standards and principles take place in contexts of discussions about cybersecurity, trade, technical standards, corporate responsibility and Internet governance. This section provides an overview of the key developments in some of the most relevant international forums.

3.2.1 The Council of Europe

While the Council of Europe (CoE) has only 47 member states, its impact on the evolution of its human rights regime reaches further. An important part of this human rights regime is the European Court of Human Rights (ECtHR) which safeguards the human rights and fundamental freedoms guaranteed in the *European Convention on Human Rights* (ECHR) also plays an important role in adapting the existing regimes to the challenges of the digital age. The right to privacy and freedom of expression are protected by Article 8 and 10 of ECHR, respectively. The 2012 ECtHR judgement in the Ahmet Yildirim v. Turkey case set an important precedent for the application of freedom of expression online within the jurisdiction of the ECtHR. As the court notes, "The Internet has become one of the principal means for individuals to exercise their right to freedom of expression today: it offers essential tools for participation in activities and debates relating to questions of politics or public interest"[17].

In 1981 the CoE adopted the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, amended in 2014, which codified data protection standards applicable to this date[18]. Established in 2001 in Budapest, the *Convention on Cybercrime* was ratified by 44 countries, but more than 100 states have aligned their national legislation to its standards[19]. Importantly, it is currently the only international agreement under which states have agreed to cooperate with regard to fighting cybercrime, but also to subject their powers and procedures "to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties" (Art.15).

Finally it should be emphasised that the Council of Europe plays a very vocal role in the area of promoting human rights as an integral part of international law. The CoE has also been very active in mainstreaming Internet and human rights issues across many different areas of their work. Thus the role of the Council of Europe is not just legal but also political in ensuring a human rights-based approach to the Internet in international law and politics.

[16] Apart from international standards mentioned here, there is a wide range of other principles, declarations and actors available too numerous to all be listed in detail here. Among those are the work carried out by the OSCE media representative, Dunja Mijatovic, the *ROAM principles* of UNESCO (Rights-based, Openness, Access, Multistakeholder), the *G8 Deauville Declaration* (2011), the *Council of Europe Declaration on Internet Governance principles* (2011) or the *COMPACT principles* of the EU Commission.

[17] Full text available here: http://hudoc.echr.coe.int/sites/eng-press/pages/search.aspx?i=001-115705#{"itemid":["001-115705"]}

[18] http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm

[19] Full text of Convention No. 185 here: http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?CL=ENG&NT=185

3.2.2 Organization for Security and Co-operation in Europe

The Organization for Security and Co-operation in Europe (OSCE) also contributes to the existing international human rights framework. With the 57 participating states, this world's largest security-oriented intergovernmental organisation introduces measures that are not legally binding, but foster cooperation between states. In December 2013, the OSCE agreed on the first set of confidence building measures (CBM) with the goal "to enhance interstate co-operation, transparency, predictability, and stability, and to reduce the risks of misperception, escalation, and conflict that may stem from the use of ICTs"[20]. Those eleven measures range from information sharing, holding consultations or dialogues and nominating contact points to encouraging adequate national legislation. The document, which explicitly links security with responsibilities to respect human rights and fundamental freedoms, is considered an important landmark for responsible state behaviour in cyberspace. A second set of CBM for cyberspace is currently under discussion between several members of the OSCE.

3.2.3 Technical organisations

While progress achieved at an intergovernmental level is important in redefining the roles and responsibilities of states in the digital sphere, standards applicable to human rights are also a subject of constant revisions within technical organisations responsible for the proper functioning of the Internet. Although those standards might appear technical in nature, there has been a growing recognition that they have important political, social and economic consequences, and as such must be considered relevant for human rights.

The Internet Society (ISOC) is an international, non-profit organisation founded in 1992 to provide leadership in Internet related standards, education, and policy to "ensure the Internet continues to grow and evolve as a platform for innovation, economic development, and social progress for people around the world"[21]. It is under the auspices of ISOC that the Internet Engineering Task Force (IETF) operates a "large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet"[22]. The technical community develops standards and protocols by issuing requests for comments (RFC) describing methods, behaviours, research, or innovations applicable to the Internet.

The Request for Comment on protecting private information known as RCF 1984 issued in 1996, for instance, recognised that security mechanisms being developed in the IETF "require and depend on the international use of adequate cryptographic technology"[23]. Under the impression of the growing concern for the right to privacy and freedom of expression, the technical community has recently reiterated its commitment to making encryption the norm for Internet traffic. The *Statement on Internet Confidentiality*, which stresses that "encryption should be authenticated where possible, but even protocols providing confidentiality without authentication are useful in the face of pervasive surveillance", was adopted by the Internet Architecture Board (IAB), a committee overseeing the IETF, in November 2014[24].

[20] Full text available here: http://www.osce.org/pc/109168?download=true
[21] See: http://www.internetsociety.org/who-we-are
[22] See: https://www.ietf.org/about/
[23] See: https://tools.ietf.org/html/rfc1984
[24] Full text available here: https://www.iab.org/2014/11/14/iab-statement-on-internet-confidentiality/

In the draft *Proposal for research on human rights protocol considerations* the IETF proposes: "Standards and protocols form the basis of the human rights enabling infrastructure of the Internet"[25]. In a one-year preliminary research a group of technical experts will further explore this idea with the aim of setting up a new IETF study group dedicated to defining procedures allowing for adequate consideration of human rights in their standards and protocols.

The Internet Corporation for Assigned Names and Numbers (ICANN), a non-profit organisation based in the US, also contributes to the international human rights framework. It is charged with the maintenance of Internet resources and several databases, including IP addresses and domain names, which are critical to the proper functioning of the Internet.

As two recent publications point out, the responsibility for upholding human rights in the process of assigning new domain names rests both on the governments participating in ICANN's decision-making process through the Government Advisory Council (GAC) and on ICANN itself as a corporate actor (Zalnieriute & Schneider, 2014; Zalnieriute, 2015)[26]. It was also suggested that ICANN should change its bylaws to make it mandatory to take human rights into account, particularly freedom of expression and non-discrimination. This is particularly important in the context of the on-going new generic Top Level Domains (gTLD) programme, under which almost 2000 applications have been filed for registering new domain names. According to experts, ICANN's current standards on 'sensitive applied-for new gTLD's' do not fully comply with the right to freedom of expression (Zalnieriute & Schneider, 2014). This is due to the classification of certain domain names as 'sensitive', which then led to a process in which new domain names such as '.xxx', '.sucks', '.gay' or '.amazon', have received objections from different members of the ICANN community. While this highlights cultural, societal and/or political sensitivities on many issues, it also infringes on the rights of domain registrants to freely express their opinion. Even more important, though, is the fact that some of these new domains were rejected on discriminatory reasons, thus potentially limiting minority communities (such as the LGBT) in their freedoms and full enjoyment of human rights.

3.2.4 Private sector

ICANN is not the only private corporation bearing some responsibility for upholding human rights standards. In fact, the role of private sector actors is crucial as many challenges related to the transition of human rights have not yet been codified in law or technical standards, but can to a certain degree be remedied by responsible business practices. Moreover, often the only legal relationship that exists between online businesses and its customers is that limited to discussing the terms of use that might or might not protect human rights and fundamental freedoms.

In particular there are numerous challenges in dealing with large multinational corporations, on which states are increasingly dependent to protect and implement human rights online. One example is Facebook that through providing the largest global social networking platform hosts all manners of content, much of which is considered radical content. Governments have argued that they "need to work with the Internet companies" (Watt & Wintour, 2015) in order to identify radical content.

[25] Full text available here: https://datatracker.ietf.org/doc/draft-doria-hrpc-proposal/

[26] Full text available here: http://www.coe.int/t/informationsociety/Source/DGI_2014_12E%20Report%20ICANN%20and%20Human%20Rights%20updated%208%20Oct%202014.pdf

Moreover private enforcement is itself often part of the problem, leading to unaccountable, non-transparent and unpredictable decisions (McNamee, 2014; York, 2010). Coupled with the challenges of the extraterritorial enforcement of human rights, the complex relationship between nation states and the globalised private sector is one of the main challenges to ensuring human rights online (Milton Mueller, 2010).

The UN Guiding Principles on Business and Human Rights outline what can be considered a "Code of Conduct" for private sector entities on how to adequately reflect human rights in their business strategies and their respective implementation. The UN Guiding Principles "are grounded in recognition of the role of business enterprises as specialized organs of society performing specialized functions, required to comply with all applicable laws and to respect human rights." Under the UN Guiding Principles, companies operating in the ICT sector are expected to adopt an explicit policy statement outlining their commitment to respect human rights both substantially and procedurally throughout their activities; and also to put in place appropriate due diligence mechanisms which identify, assess, and prevent any adverse impact on human rights[27].

The Organisation for Economic Co-operation and Development (OECD) Guidelines for Multinational Enterprises further explain that "[a] State's failure either to enforce relevant domestic laws, or to implement international human rights obligations or the fact that it may act contrary to such laws or international obligations does not diminish the expectation that enterprises respect human rights. In countries where domestic laws and regulations conflict with internationally recognized human rights, enterprises should seek ways to honour them to the fullest extent which does not place them in violation of domestic law"[28].

According to its mission statement, the Global Network Initiative[29] aims to create "a collaborative approach to protect and advance freedom of expression and privacy in the ICT sector", since governmental pressure is increasing to comply with domestic laws and policies which are deemed in conflict with human rights.

In conclusion, responses to digital human rights challenges inevitably involve the corporate sector; however, this dependency on corporate actors to reach solutions is also part of the problem. There is no denying that the corporate sector can contribute to the promotion and protection of human rights. At the same time there are many situations in which corporations need to do more in order to ensure that human rights are enshrined as a central part of rights online.

3.2.5 Multistakeholder meetings

While governments, technical community, private sector and civil society each have a unique role and responsibility in protecting human rights online, there has been a growing understanding that only norms developed and adapted with the involvement of all these actors can adequately respond to challenges confronted by users of technologies. As a result, the practice of 'multistakeholder' development of laws, principles and policies has gained significant traction in international debates.

A selling example of such bottom-up, open and participatory process is the NETmundial Conference, which took place in Sao Paulo in April 2014. Thousands of participants representing a variety of stakeholders endorsed the *NETmundial Multistakeholder Statement,* which reiterates that Internet

[27] Full text available here: http://shiftproject.org/sites/default/files/GuidingPrinciplesBusinessHR_EN.pdf
[28] Full text available here: http://www.oecd.org/daf/inv/mne/48004323.pdf
[29] Full text of principles available here: https://globalnetworkinitiative.org//principles/index.php

governance principles should be underpinned by universal human rights[30]. The affirmation that "[R]ights that people have offline must also be protected online" in accordance with international human rights expressed in the UN 2012 resolution is echoed in the Statement. The specific rights named include freedom of expression as well as the right to privacy, which is specified as "not being subject to arbitrary or unlawful surveillance, collection, treatment and use of personal data."

Significantly, the NETmundial conclusions also include other human rights affected in the digital sphere, namely freedom of association: "Everyone has the right to peaceful assembly and association online, including through social networks and platforms." It elaborates on freedom of information and access to information by stating, "Everyone should have the right to access, share, create and distribute information on the Internet, consistent with the rights of authors and creators as established in law." It points to the specific needs of persons with disabilities by promoting accessibility of online resources. Finally, it explicitly links human rights with development debates by stating that Internet "is a vital tool for giving people living in poverty the means to participate in development processes"[31].

The results of the NETmundial are a reflection of the need to expand the scope of human rights considerations beyond freedom of expression and the right to privacy to other human rights. It is also remarkable that the words 'individual' and 'user of the Internet' are more and more often applied interchangeably to describe the subject of human rights safeguards. This individual component stressed in multistakeholder discussions supports the narrative shift towards human rights.

When studying existing human rights law it should be obvious that there is no lack of norms. What is lacking is the trust that these fundamental normative frameworks are not adequately respected, safeguarded and promoted. Human rights are evolving over time and while some technological developments certainly pose challenges for their protection, these are not insurmountable. In order to ensure a successful evolution of human rights norms and standards, it seems crucial that future developments of human rights are discussed broadly and involving all concerned actors.

[30] NETmundial statement available here: http://netmundial.br/netmundial-multistakeholder-statement/

[31] NETmundial statement available here: http://netmundial.br/netmundial-multistakeholder-statement/

4 Policy initiatives promoting the transition of human rights

Ultimately though, no laws or guidelines can address all the challenges created by digital developments. In order to adequately protect digital rights, countries need to cooperate and develop comprehensive and smart policies to fulfil their obligations set out in internationally agreed laws and standards. There is also a need for leadership from the corporate sector to ensure that corporate compliance and due diligence mechanisms promote and protect human rights. This section will attempt to evaluate several international policy initiatives and their current potential to protect and promote digital rights.

4.1 Exports controls in the Wassenaar arrangement

Export controls are becoming an important mechanism for implementing human rights-based approach in international policy. However, due to a lack of international coordination and oversight, existing measures have been inadequate in preventing export of censorship and surveillance technologies to countries where human rights are systematically abused (Maurer, Omanovic, & Wagner, 2014).

The Wassenaar Arrangement is one such forum where coordination takes place, although it is focused on international security and stability and does not explicitly mention human rights issues. Listings are updated annually, yet it takes time for technologies used for censorship and surveillance to be included (Maurer, Omanovic, et al., 2014). In December 2013, the Wassenaar Arrangement agreed to include some surveillance technologies in the dual-use lists[32]. While some surveillance technologies such as types of mass surveillance, targeted surveillance and IMSI catchers are included in the current Wassenaar lists; the definitions still need to be adapted to ensure they cover the right technologies.

In particular the negotiation of the actual control lists used in Wassenaar is a cause for concern. Negotiations take place in private between a few governmental experts with little transparency about the decision-making processes, which also challenges both the accountability of Wassenaar as a whole. While civil society and investigative journalists have played an important role in monitoring the sale of unlicensed technologies, Wassenaar signatory states need to increase institutional transparency by opening up their decision making processes and integrating civil society actors as relevant actors and experts in the negotiation process.

4.2 Internet governance and the WSIS process

The World Summit on Information Society (WSIS), which took part in two phases in 2003 in Geneva and 2005 in Tunis, declared that it is crucial to pay particular attention to ICTs and other technological developments to ensure that we live in "a people-centred, inclusive and development-oriented Information Society"[33]. These two summits initiated a ten-year process for the implementation of a range of different action lines to help achieve this goal. The human rights-based component is comparatively strong in this process as the focus lies on the empowerment of individuals, policies for access, affordability and inclusive participation.

The "WSIS+10-Review" which will take place in December 2015 in New York in the margins of the United Nations General Assembly may pave the way to a renewed commitment to an inclusive and

[32] Full list of controlled/listed technologies, incl. dual-use can be found here: http://www.wassenaar.org/controllists/2014/WA-LIST%20%2814%29%201/WA-LIST%20%2814%29%201.pdf

[33] See WSIS Declaration of Principles here: http://www.itu.int/wsis/docs/geneva/official/dop.html

rights-based Internet Governance regime. However the ongoing conflict about the missing governance in Internet Governance (van Eeten & Mueller, 2012) raises questions about the utility of the WSIS process.

The challenge then is, to ensure that every future development takes human rights into account adequately. Here extending the mandate of the Internet Governance Forum (IGF) at the end of 2015 by the second committee of the United Nations could also be helpful. Any such an extension should also ensure that the IGF actually responds to many of its critics (Milton Mueller & Wagner, 2014).

4.3 Freedom Online Coalition

The Freedom Online Coalition is an international coalition of states composed of 26 governments from a mix of developed and developing countries, of which 12 are from Europe. The FOC coordinates diplomatic efforts to support free expression, association, assembly, and privacy online. Those efforts include sharing information, issuing joint démarches and diplomatic notes in case of suspected violations of human rights online and formulating common public statements, declarations and positions in international negotiations. In October 2014, the Coalition has called on governments and businesses to curb use of surveillance technology in an international, multi-stakeholder effort, which "should include the development of appropriate and consistent national laws and policies governing the use and export of such technologies" (FOC, 2014). At the same time it has been suggested that the FOC has been used as a shield to deflect criticism about human rights violations by the governments involved; Mongolia is purportedly a FinFisher customer (Marquis-Boire, Marczak, Guarnieri, & Scott-Railton, 2014), the UK and the U.S. are both part of the five eyes (Nyst & Crowe, 2014).

4.4 Technological sovereignty measures

In an impulse to shield their citizens from mass surveillance many governments have called for measures to protect "technological sovereignty". In practice, this has meant forcing private service providers to nationalise their operations and thereby attempt to ensure that the government has greater control over the data stored there. Although a reference to human rights, in particular the right to privacy is often used to justify such measures, they also signal a trend to revert to a state-centric national security perspective. While it is understandable that states would try to gain greater control over sensitive data, only when states actually increase human rights standards when localising data, can such moves be considered legitimate.

Several European policy makers and companies have proposed data localisation requirements, local routing of internet traffic or national email, but have so far not received widespread support (Maurer, Morgus, Skierka, & Hohmann, 2014). These range from national routing in Germany that was proposed by private and public actors in Germany (Abboud & Maushagen, 2013) to proposals for new submarine cables between Europe and Latin America by the President of the European Council, Herman Van Rompuy[34] or by Finnish Minister of Education and Communications, Krista Kiuru, who wanted "Finland to be a safe harbour for data"[35]. Outside of Europe the Brazilian government was one of the first to explore the requirement for foreign companies to store data within its national borders, but eventually dropped this provision from the final text of its 'Marco Civil da Internet', the 'bill of Internet rights' adopted in 2014. Data localisation measures in Russia, on the contrary, are scheduled

[34] See http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/141144.pdf for further details.

[35] See http://www.lvm.fi/pressreleases/4402744/minister-kiuru-on-submarine-cable-decision-finland-to-be-a-safe-harbour-for-data for further details.

to enter into force in September 2015. Similar measures have historically been pursued by both the Chinese and Iranian governments to ensure that as much data as possible is localised within their national borders (Jiang, 2012; Rhoads & Fassihi, 2011).

Although such measures offer the promise of increasing security and privacy of digital communications, they can in fact have the adverse effect of increasing the capacity of governments to monitor and/or control their citizens (Maurer, Morgus, et al., 2014). Authoritarian regimes have long pursued measures that, on the one hand, effectively shield their citizens from communication with the outside world, and, on the other hand, allow them to monitor their activities online. A state-controlled *intra*net is promoted – although not always implemented - in Cuba, Iran and North Korea, where the governments block content deemed inappropriate; this is then called "national Internet" or "halal Internet" (B. Hoffmann, 2012; Rahimi, 2011).

4.5 Extraterritorial application of human rights

As governments seek to increase control over citizens and their data within their countries' territories, scholars point to the growing importance of the extraterritorial application of human rights. As Marko Milanovic argues, "[I]n the age of globalization states are increasingly affecting the human rights of individuals outside their borders, and that this explains both the increase of litigated cases on extraterritorial application and the growing importance of the issue generally" (Milanovic, 2011).

Extraterritorial application of human rights is a concept that argues for the expansion of states human rights obligations beyond their own borders. While many states have resisted the extraterritorial application of their human rights obligation, legal scholars (Milanovic, 2011) and the UN Human Rights Council (La Rue, 2013) tend to agree that at least some form of extraterritorial applicability exists. In his report UN Special Rapporteur La Rue stated that "a number of States have begun to adopt laws that purport to authorize them to conduct extra-territorial surveillance or to intercept communications in foreign jurisdictions. This raises serious concern with regard to the extra-territorial commission of human rights violations and the inability of individuals to know that they might be subject to foreign surveillance, challenge decisions with respect to foreign surveillance, or seek remedies" (La Rue, 2013). In consequence it remains to be hoped that both states and the private sector will treat their human rights obligations as truly universal, rather than privileging the digital rights of their citizens over those of non-citizens (Bowden, 2013).

4.6 Technical solutions promoted by international policies

Strong encryption has long allowed activists, investigative journalist and researchers to protect sensitive communication, but it is often considered too cumbersome to be used by the wider population. Making encryption accessible to more users around the world has motivated engineers and private sector to introduce encryption as a default standard for Internet protocols, software and hardware.

However, there have also been concerns among the intelligence community that increased use of encryption might hinder intelligence efforts, a phenomenon that is sometimes termed 'going dark.' The argument is that greater public use of strong end-to-end encryption risks limiting intelligence services ability to do their job (Yadron, 2015). However, similarly to many debates about national security policy there is very little empirical evidence or substantial academic research to justify such claims. In response many critics suggest limiting public access to encryption or building back doors into such technologies make them 'defective by design' and that such access will inevitably be abused (Bauman et al., 2014; Greenwald, 2014; Johnson, Maillart, & Chuang, 2014). Importantly even greater use of encryption within society does not necessarily prevent targeted surveillance, but it does make mass surveillance a lot more difficult and costly. Finally it should also be noted that the debate on the regulation of cryptography is not a recent phenomenon but is a debate that has been going on for decades[36].

5 EU actions and policies and their impact

The EU has engaged in numerous measures related to Internet and human rights issues in recent years. Following the Arab uprisings in 2011 and Snowden leaks in 2013 the issue has grown in prominence, leading to increasing political interest.

5.1 EU external policy initiatives

The release of the *EU Human Rights Guidelines on Freedom of Expression Online and Offline* in 2014 was an important step to recognising the importance of digital communications in the EU's foreign policy strategy. While the title explicitly focuses on freedom of expression, the guidelines extend to topics of privacy, surveillance and even EU public diplomacy. One particularly important element of these Guidelines is the section on Financial Instruments, which explicitly recommends "All appropriate EU external financial instruments should be used to further protect and promote freedom of opinion and expression online as well as offline, including by supporting the emergence of a free, diverse and independent media"[37]. Another important mechanism is the European Instrument for Democracy and Human Rights (EIDHR), and its small grants mechanism for individuals facing immediate threats.

Importantly, the European Parliament adopted a resolution on the Digital Freedom Strategy in the EU Foreign Policy (P7_TA(2012)0470) in 2012 and explicitly "stresses that the promotion and protection of digital freedoms should be mainstreamed" and "[c]alls for a ban on exports of repressive technologies and services to authoritarian regimes"[38]. Another key resolution by the European Parliament that strongly affected external relations is the resolution on the Suspension of the SWIFT agreement as a result of NSA surveillance (P7_TA(2013)0449). As many of the security commitments made by Europe were called into question by extensive revelations of NSA surveillance, this resolution was an important signal that Europe was also prepared to take concrete steps to limit the sharing of data between Europe and the U.S. It needs to be seen in the context of European Parliament resolutions of 4 July 2013 (P7_TA(2013)0322) and 12 March 2014 (P7_TA(2014)0230) which both focus on the revelations of NSA surveillance and its impact on EU citizens' fundamental rights.

The latter two resolutions in particular draw attention to the surveillance bodies in EU Member States and calls for a "European Digital Habeas Corpus." The resolutions also include a far-reaching action plan with proposals like for the EU to "Suspend Safe Harbour until a full review has been conducted and current loopholes are remedied" (P7_TA(2014)0230). It remains to be seen what consequences this ambitious European Digital Habeas Corpus action plan will have.

The European Parliament has also organised regular hearings and events that emphasize privacy and digital rights as well as the harms caused by mass surveillance. By putting a strong emphasis on

[36] See http://openpgp.vie-privee.org/gilc-wass-fr.htm for further details.

[37] See http://eeas.europa.eu/delegations/documents/eu_human_rights_guidelines_on_freedom_of_expression_online_and_offline_en.pdf for further details.

[38] See http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2012-0470+0+DOC+XML+V0//EN for further details.

privacy and data protection, the European Parliament's position ensures that privacy is debated as one of the key Internet and human rights issues both inside and outside of the Europe[39].

Finally the new *EU Global Digital Strategy* is currently being discussed within the European Commission that is to be published in May 2015. It remains to be seen if it will be an important stem in implementing a global strategy firmly embedded in human rights-based approach.

Another area where the EU regularly addresses human rights concerns in a digital context is human rights dialogues such as those with Turkmenistan and China. There has been some concern about the efficacy of such mechanisms as well as the fact that they may lead to human rights only being discussed within this policy silo and not anywhere else (Boonstra & Laruelle, 2013; K. Hoffmann, 2010; Kinzelbach, 2014).

Thus it is to be welcomed that the "promotion and protection of human rights online"[40] are also part of the broader U.S.-EU cyber-dialogue, as well as the Council of the European Union conclusions on Internet Governance which explicitly emphasizes "human rights and democratic values" (16175/14) and suggests that "Internet can be a tool for promoting human rights globally" (16200/14). However, it is important to ensure that human rights are included in the upcoming diplomatic conclusions on 'cyber' being prepared by the EEAS as well as mainstreaming Internet & human rights knowledge into training programs for EEAS staff.

Another important venue for EU's external policy strategy is the European Neighbourhood Policy (ENP) and Enlargement negotiations. The consultations of the ENP launched by the European Commission present an opportunity to promote human rights-based approach in 16 neighbouring countries, also in the digital sphere[41]. With a budget of €15.4 billion for the period 2014-2020, the new European Neighbourhood Instrument (ENI) creates an incentive-based approach on the basis of progress of individual countries towards democracy and respect of human rights. Implementation of human rights in the digital sphere can and should be an important criterion in measuring this progress.

In a similar vein, negotiations with candidate countries Albania, Macedonia, Iceland, Montenegro, Serbia and Turkey, as well as potential candidates Bosnia and Herzegovina and Kosovo could be a venue for EU to promote human rights-based approach. The second edition of Instrument for Pre-accession Assistance (IPA II), with a budget of EUR 11.7 billion for the period 2014-2020 for developments in area such as democracy, governance and rule of law, should also cover the digital rights component.[42] As negotiations unfold in the coming years, the EU can use the framework of negotiations and the 'Copenhagen criteria', which explicitly reference human rights, to address challenges to human rights in the digital sphere in these countries.

5.2 Digital rights strategies within the EU

The main legislation that governs 'digital rights' in Europe is the Charter of Fundamental Rights, which came into force along with the treaty of Lisbon in 2009. The Charter provides a foundation for

[39] See http://www.europarl.europa.eu/news/en/news-room/content/20150116IPR09941/html/Committee-on-Human-Rights-meeting-21-01-2015-15001630 for further details.

[40] See http://eeas.europa.eu/statements-eeas/2014/141205_05_en.htm for further details.

[41] The ENP was designed in 2003 to develop closer relations between the EU and its neighbouring countries. It covers to the South: Algeria, Egypt, Israel, Jordan, Lebanon, Libya, Morocco, Palestine, Syria and Tunisia; to the East: Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine. See http://ec.europa.eu/enlargement/news_corner/news/2015/03/20150304_en.htm for further details.

[42] See http://ec.europa.eu/enlargement/instruments/overview/index_en.htm for further details.

European positions on digital rights, such as the 2014 judgement of the European Court of Justice (ECJ) that the EU Data Retention Directive is invalid[43]. Beyond the Charter there are also soft law measures, such as for instance the Code of EU Online Rights published by the European Commission in 2012. While the Code is focused on the basic consumers' rights in EU legislation, it serves as an example of how the EU can facilitate transition of different policy areas and harmonisation between Member States[44].

One of the key legislative initiatives related to digital rights issues in Europe is the reform of the data protection framework. The reform is still under discussion, but the resolution adopted by the European Parliament on 12 March 2014 (P7_TA(2014)0212) indicates a willingness of the MEPs to adapt the legislative framework to protect privacy in the digital sphere. Public debates about specific elements of the new EU General Data Protection Regulation, such as rights of individuals to remove personal data, or individual and collective rights to sue in response to breaches of regulation, have thus far supported a narrative shift towards human rights. The debate has already considerably contributed to the international understanding of what privacy *is* and how data protection regulations can be used to protect human rights in the digital sphere. However, it remains to be seen what the final shape of the regulation and its impact on regulatory frameworks beyond Europe will be.

In parallel with the debate on reform of data protection framework, a new EU Directive concerning measures to ensure a high common level of network and information security across the Union (NIS) is also under discussion. The aim of the directive is improving the security of the Internet and the private networks and information systems by requiring the Member States to increase their preparedness and improve their cooperation with each other, and by requiring operators of critical infrastructures[45].

The proposal of the directive accompanied the EU Cybersecurity Strategy designed by High Representative Catherine Ashton and the European Commission. The Communication "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace" adopted by the EU in 2013, is the first comprehensive EU policy document on internal market, justice and home affairs and foreign policy aspects of cyberspace issues.

The Strategy emphasises that fundamental rights, democracy and the rule of law as enshrined in the Charter of Fundamental Rights of the European Union need to be protected in cyberspace. It also explicitly states: "Increased global connectivity should not be accompanied by censorship or mass surveillance"[46]. However, the terminology of 'cyber' and 'security', serves to securitize and militarize digital communications rather than to emphasize their civilian component. While there is evidently a tension between digital rights and national security, the European Parliament, the Commission, the Council and the Member States should wherever possible avoid using this terminology, because it shifts attention from the Internet as global common good to Internet as a military battlefield. Some argue that military rhetoric about the Internet can even lead down the slippery slope of a digital cold war (M. Mueller, 2013).

Moving from rhetoric to strategies, the "No Disconnect Strategy" developed by former Commissioner Kroes at DG CNECT was intended to "uphold the EU's commitment to ensure human rights and

[43] See http://www.loc.gov/law/help/eu-data-retention-directive/eu.php for further details.
[44] See http://ec.europa.eu/digital-agenda/en/code-eu-online-rights for more details.
[45] See http://eeas.europa.eu/top_stories/2013/070213_cybersecurity_en.htm for more details.
[46] See http://eeas.europa.eu/policies/eu-cybersecurity/cybsec_comm_en.pdf for more details.

fundamental freedoms are respected both online and off-line, and that internet and other information and communication technology (ICT) can remain a driver of political freedom, democratic development and economic growth"[47].

There has been little progress on the Strategy despite the initial fanfare. One of the few tangible results is a feasibility study for a European Capability for Situation Awareness (ECSA), which can be seen as an attempt to provide the EU Commission with better information about digital rights violations on the ground. While a feasibility study is still ongoing it remains unclear whether such a platform will actually be developed[48].

Given that a new European Commission has recently been appointed, it will be important to see how the two new Vice Presidents Andrus Ansip and Federica Mogherini collaborate on this issue. It would doubtless be helpful if different elements of EU strategic policy on human rights and digital policy were better integrated and if the *EU Human Rights Guidelines on Freedom of Expression Online and Offline,* the No Disconnect Strategy, ECSA as well as the *Review of European Export Control Policy* were better coordinated.

Lastly, there is the more general issue of the EU's credibility in promoting Internet and human rights when EU member states are criticised for violating them, too. Analysing Hungary's new media laws, for instance, Human Rights Watch concluded that these "undermine judiciary [and] media"(HRW, 2014). Others are swift to point out the UK's role in the 'five eyes' alliance (Nyst & Crowe, 2014). Here the challenge for the EU and its member states is to improve the coherence between their internal and external policies. It is very challenging for EU member states to infringe on key human rights provisions while at the same criticising states outside the EU for similar violations.

The EU should improve its credibility in these areas by considering problems at home. Nevertheless while some member state policies may prove challenging for a human rights agenda, these should not prevent the EU from pushing further. Instead, in order to live up to a coherent foreign policy, the EU should emphasise those aspects where it still has to increase efforts to ensure that it pursues a rights-based agenda in foreign policy.

5.3 Export controls in the EU: Wassenaar arrangement and beyond

One area where the EU has been particularly active is the area of export controls of surveillance technologies. In December 2011, following extensive media reporting about a European consortium delivering surveillance technologies to Syria (Elgin & Silver, 2011), the Council of the European Union updated existing sanctions on Syria to prevent the trade in "equipment and software intended for use in the monitoring of the Internet and telephone communications" (17985/11).

To this date, the EU has only included surveillance technology in its restrictive measures targeting Syria and Iran, but not across all existing restrictive measures. The EU also prohibits export of equipment that might be used for internal repression as part of measures targeting Belarus, Cote d'Ivoire, Republic of Guinea, Libya, Myanmar (Burma), and Zimbabwe (Maurer, Omanovic, et al., 2014).

In response to many of these problems, EU member states have become some of the main proponents of stronger regulation of surveillance technologies on the level of the Wassenaar Arrangement. While these changes are by no means perfect, they are an important first step in regulating the export of surveillance technologies (Maurer, Omanovic, et al., 2014). At the EU level

[47] See: http://europa.eu/rapid/press-release_IP-11-1525_en.htm?locale=en
[48] The lead author of this report Dr. Ben Wagner is also on the ECSA advisory board.

these developments have been flanked by a *Review of European Export Control Policy*, which explicitly discusses a regulation of "cybertools for mass surveillance, monitoring, tracking and interception" (COM(2014) 244).

5.4 Trade and investment negotiations with EU partners

There has been an on-going debate about EU policies in regard to trade and digital rights, as there seems to be an on-going conflict between human rights policy aspirations and actual agreements. This is particularly obvious in regard to the EU-U.S. Safe Harbour agreement, but also in regard to the TTIP and TiSA negotiations.

With 50 trade agreements already in place and many more currently negotiated, the EU is well positioned to continue to use bilateral and investment agreements as a trigger for incentives for protection of human rights in partner countries through human rights clauses. Implementation of core conventions on human rights is rewarded with additional trade incentives under GSP+, a component of the EU Generalised Scheme of Preferences ('GSP'). This includes the implementation of the ICCPR and 26 other core conventions, which can contribute considerably to promoting and strengthening digital rights in GSP+ countries. Participating countries include Armenia, Bolivia, Cape Verde, Costa Rica, Ecuador, El Salvador, Georgia, Guatemala, Mongolia, Panama, Paraguay, Pakistan and Peru. It is important to ensure that sustainability and good governance criteria are implemented in the GSP+ agreements in a way that promotes and protects human rights. For example Pakistan has a long history of disconnection Internet & telecommunications networks and yet it is unclear whether the EU or the EU Special Representative for Human Rights has raised this matter with the Pakistani government in regard to GSP+ compliance.

Human rights are also at the core of the European Neighbourhood Partnership (ENP) and the Cotonou Agreement with ACP countries. In consequence, transparency and public involvement in EU partnership and trade negotiations through public consultations, civil society dialogue and sustainability impact assessment should be used as a platform to raise concerns about infringements of digital rights in partner countries.

6 Areas for discussion and ways forward

First and foremost it should be noted that there is a need for a broad approach to human rights. The overt focus on censorship and surveillance has masked many other human rights based approaches that are equally relevant. While we have attempted to provide additional examples, this study too suffers from a bias towards censorship and surveillance. It remains an ongoing challenge to broaden the focus of this debate and demonstrate the numerous number of rights affected. This inevitably means mainstreaming digital rights across all sectors, as there is arguably no area of human rights not affected by the ongoing shift to digital technologies.

Based on our previous analysis we propose the following recommendations to the DROI Subcommittee on Human Rights at the European Parliament:

1. Encourage EU to further promote protection of human rights in national legislation of the third countries through capacity building and technical assistance. While much of the debate on human rights has focussed on international agreements, this cannot substitute national legislative frameworks. Furthermore, EU member states should develop models for human rights-based legislation in areas such as lawful interception, privacy protection and the rule of law in cyberspace and share this with their partners around the world.

2. Strengthen accountability across all areas of digital rights. The lack of clear accountability means that individuals must often seek redress from private rather than public actors. A push to reduce costs or administrative burdens cannot justify compromising on rights. The EU should support the creation of better individual redress and appeal mechanisms for privacy and other digital rights violations in front of the ECHR and other relevant judicial authorities inside and outside of Europe.

3. Improve transparency by both private companies and governments. The EU should demand greater transparency of both algorithms and institutions[49] and ensure that the EU has access to key information about how digital technologies are shaping human rights. Much of this information is not available to academia, journalists, the general public or even relevant public regulators and thus cannot be effectively evaluated.

4. Draft comprehensive digital policies and strategies. Although this is already being conducted to some extent, the "digital component" should be further mainstreamed into any future EU strategy or policy, thereby ensuring that policies are drafted with a human rights-based approach in mind. In particular the European Neighbourhood Partnership (ENP) and EU Development Cooperation could benefit from a greater focus on digital rights.

5. Deepen strategic collaboration on digital rights issues of EU and its member states with Latin America. While the 'Privacy Resolution' of Brazil and Germany and a new European-Latin American Internet cable are important first steps, there are many additional areas where potential collaboration should be explored. These include greater exchange between European and Latin American CERTs, data protection agencies, diplomatic communities and judicial authorities as well as stronger business and research collaboration between the two continents.

6. Build further institutional knowledge on digital rights issues within international EU policy-making, in particular the EU missions across the world**.** For the human rights contact points at EU

[49] See https://cihr.eu/the-ethics-of-algorithms/ for further details

missions a regular digital rights training should become mandatory. Moreover, missions and directorates should be able to allow for secure communication in situations and regions where this can be pivotal to the safety of individuals.

7. Further promote comprehensive independent research on human rights and technology and strengthen European research collaboration in these areas**.** While private sector collaboration is to be welcomed, the existing massive reliance on corporate funding for research in this area challenges the integrity and quality of research being produced.

8. De-militarise 'Cyber'. The narrative shift towards human rights could ensure that the EU explicitly focuses on a civilian rather than a military dimension of its Internet policies and strategies. This will be particularly important in the upcoming *EU Global Digital Strategy* where the European Parliament will need to ensure that human rights and not 'cyber security' take centre stage.

9. Bring forward human rights aspects in trade as a key mechanism to ensure the acceptance of international trade agreements and EU trade policy. This involves fine-tuning existing export controls of surveillance technologies where Europe needs to become a leading actor in emphasising human rights as well as promoting a stronger digital rights evaluation mechanism with GSP+ trade frameworks.

10. Support human rights-enhancing technologies by further deregulating cryptography at international and national levels, in particular in the Wassenaar Arrangement but also by creating exemptions in the EU dual-use regulation through the mechanism of a General Export Authorisation for cryptography (GEA). There is also a need for further research and training in this area to ensure that the societal infrastructure that enables secure communication is functional, easy-to-use and better understood by European citizens.

11. Encourage EU member states to push for a new General Comment to Article 17 on the Right to Privacy at the Human Rights Committee at the United Nations. This will help to ensure that interpretations of international law are relevant for the digital age while also clarifying state responsibilities in regards to the Right to Privacy. In a similar vein, EU member states should also support the establishment of a United Nations Special Rapporteur on the Right to Privacy.

Bibliography

Abboud, L., & Maushagen, P., Germany wants a German Internet as spying scandal rankles, *Reuters*, 2013. Retrieved March 05, 2015, from http://www.reuters.com/article/2013/10/25/us-usa-spying-germany-idUSBRE99O09S20131025

Arce, N., Cyber Attack Bigger Threat Than ISIS, Says U.S. Spy Chief. *Tech Times*, 2015. Retrieved March 06, 2015, from http://www.techtimes.com/articles/35965/20150227/cyber-attack-bigger-threat-than-isis-says-u-s-spy-chief.htm

Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D., & Walker, R. B. J., After Snowden: Rethinking the Impact of Surveillance. *International Political Sociology*, *8*(2), 121–144. doi:10.1111/ips.12048, 2014.

Bennett, Colin J. Haggerty, K., *Security Games: Surveillance and Control at Mega-Events* (p. 208). Routledge, 2012.

Bequelin, N., Jailing of Ilham Tohti Will Radicalize More Uighurs - NYTimes.com, 2014. Retrieved January 14, 2015, from http://www.nytimes.com/2014/09/26/opinion/nicholas-bequelin-china-jailing-of-ilham-tohti-will-radicalize-more-uighurs.html?_r=0

Birnbaum, M., Russian blogger law puts new restrictions on Internet freedoms. *Washington Post*, 2014. Retrieved February 15, 2015, from http://www.washingtonpost.com/world/russian-blogger-law-puts-new-restrictions-on-internet-freedoms/2014/07/31/42a05924-a931-459f-acd2-6d08598c375b_story.html

Boonstra, J., & Laruelle, M., EU-US cooperation in Central Asia: parallel lines meet in infinity? *EUCAM Policy Brief*, 2013.

Bowden, C., *The US surveillance programmes and their impact on EU citizens' fundamental rights*. Brussels, Belgium, 2013.

Cavelty, M. D., From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. *International Studies Review*, 2014.

Ctizen Lab. Morgan Marquis-Boire, Marczak, Bill Claudio Guarnieri, and J. S.-R., You Only Click Twice: FinFisher's Global Proliferation - Citizen Lab, 2013. Retrieved January 09, 2015, from https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2/

Culzac, N., Iranians behind Tehran version of "Happy" sentenced to six months in prison and 91 lashes - Middle East - World - The Independent, *The Independent*, 2014. Retrieved January 14, 2015, from http://www.independent.co.uk/news/world/middle-east/iranians-behind-tehran-version-of-happy-sentenced-to-six-months-in-prison-and-91-lashes-9741014.html

Deibert, R. J., Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace. *Millennium - Journal of International Studies*, *32*(3), 501–530. doi:10.1177/03058298030320030801, 2003.

Dunn Cavelty, M., Cyber-security and threat politics: US efforts to secure the information age, 2007.

Elgin, B., & Silver, V., Syria Crackdown Gets Italy Firm's Aid With U.S.-Europe Spy Gear - Bloomberg. *Bloomberg*, 2011.

Epstein, G., Online and Off, Information Control Persists in Turkey. *Electronic Frontier Foundation*, 2013. Retrieved June 24, 2014, from https://www.eff.org/deeplinks/2013/07/online-and-information-control-persists-turkey

Feenberg, A., *Questioning Technology* (p. 264). Routledge, 1999.

FIDH, *Surveillance Technologies "Made in Europe". Regulation Needed to Prevent Human Rights Abuses*, 2014.

Finn, P., Cyber Assaults on Estonia Typify a New Battle Tactic. Washington: Washington Post, 2007. Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802122.html

FOC, Freedom Online Coalition: Statement on the Use and Export of Surveillance Technology, 2014. Retrieved January 14, 2015, from https://www.freedomonlinecoalition.com/wp-content/uploads/2014/10/2-FOC-Joint-Statement-on-the-USe-and-Export-of-Surveillance-Technology-October-2014.pdf

Freedman, L., Censorship and manipulation of family planning information: an issue of human rights and women's health. *Health and Human Rights: A Reader*, 1999.

Greenwald, G., *No place to hide: Edward Snowden, the NSA, and the US surveillance state*, 2014.

Hoffmann, B., Civil society in the digital age: how the Internet changes state-society relations in authoritarian regimes. The case of Cuba. In Francesco Cavatorta (Ed.), *Civil Society Activism under Authoritarian Rule. A comparative perspective* (pp. 219–244). London, New York: Routledge, 2012.

Hoffmann, K., The EU in Central Asia: successful good governance promotion? *Third World Quarterly*, 2010.

HRW, Hungary. *Human Rights Watch,* 2014. Retrieved January 06, 2015, from http://www.hrw.org/europecentral-asia/hungary

Jenkins, P. N., Turkey Lifts Two-Month Block on YouTube | TIME, 2014.

Jiang, M., Authoritarian informationalism: China's approach to Internet sovereignty. *Forthcoming in P. O'Neil. & R. Rogowski (Eds.), …, 30*(2), 71–89. doi:10.1353/sais.2010.0006, 2012.

Johnson, P., Maillart, T., & Chuang, J., Government Surveillance and Incentives to Abuse Power. In *Workshop on the Economics of Information Security (WEIS)*. Pennsylvania State University, 2014.

Kinzelbach, K.,*The EU's Human Rights Dialogue with China: Quiet Diplomacy and Its Limits* (p. 236). Routledge, 2014.

Korff, D., *Expert Opinion prepared for the Committee of Inquiry of the Budestag into the SEYES global surveillance systems revealed by Edward Snowden*. Berlin, Germany, 2014.

La Rue, F., *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue (A/HRC/23/40)*. Geneva, 2013.

Lab, C.,*You Only Click Twice: FinFisher's Global Proliferation - Citizen Lab*, 2013.

Lab, K., *Syrian Malware, the ever-evolving threat*, 2014.

LaFrance, A., Where Design Choices and Civil Rights Overlap - The Atlantic. *The Atlantic*, 2015. Retrieved January 14, 2015, from http://www.theatlantic.com/technology/archive/2015/01/where-design-choices-and-civil-rights-overlap/384142/

LGBT Technology Partnership, Homosexuality, Internet Censorship and Silence » LGBT Technology Partnership, 2013. Retrieved February 15, 2015, from http://lgbttechpartnership.org/homosexuality-internet-censorship-and-silence/

Livingstone, S., Digital Media and Children's Rights. *LSE Media Policy Project*, 2014. Retrieved from http://blogs.lse.ac.uk/mediapolicyproject/2014/09/12/sonia-livingstone-digital-media-and-childrens-rights/

Marczak, B., Guarnieri, C., Marquis-Boire, M., & Scott-Railton, J., *Mapping Hacking Team's "Untraceable" SpywareMapping Hacking Team's "Untraceable" Spyware*, 2014.

Marquis-Boire, M., Marczak, B., Guarnieri, C., & Scott-Railton, J., For Their Eyes Only: The Commercialization of Digital Spying, 2014. Retrieved January 14, 2015, from https://citizenlab.org/storage/finfisher/final/fortheireyesonly.pdf

Marthews, A., & Tucker, C., Government Surveillance and Internet Search Behavior. *SSRN Electronic Journal*. doi:10.2139/ssrn.2412564, 2014.

Maurer, T., Morgus, R., Skierka, I., & Hohmann, M., Technological Sovereignty: Missing the Point?, 2014. Retrieved January 14, 2015, from http://www.gppi.net/fileadmin/user_upload/media/pub/2014/Maurer-et-al_2014_Tech-Sovereignty-Europe.pdf

Maurer, T., Omanovic, E., & Wagner, B., *Uncontrolled Global Surveillance: Updating Export Controls to the Digital Age*. Washington D.C., 2014.

McCarthy, D. R., Open Networks and the Open Door: American Foreign Policy and the Narration of the Internet. *Foreign Policy Analysis*, 2011.

McNamee, J., ENDitorial: Turkish censorship - Swedish built, by royal appointment » EDRi. *edri*, 2014. Retrieved July 14, 2014, from http://edri.org/enditorial-turkish-censorship-built-sweden-royal-appointment/

Milanovic, M., *Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy* (p. 276). Oxford University Press, 2011.

Mueller, M., *Networks and States: The Global Politics of Internet Governance* (p. 280). MIT Press, 2010.

Mueller, M., *Are we in a Digital Cold War. Internet Governance Project*. Syracuse, N.Y., 2013.

Mueller, M., & Wagner, B., *Finding a Formula for Brazil: Representation and Legitimacy in Internet Governance* (No. 1). Internet Policy Observatory Working Paper Series, University of Pennsylvania, Annenberg School, 2014.

Nyst, C., & Crowe, A., *Unmasking the Five Eyes' global surveillance practices. GISWatch*. Johannesberg, 2014.

Pasquale, F., *The Black Box Society: The Secret Algorithms That Control Money and Information* (p. 319). Harvard University Press, 2015.

Pillay, N., The right to privacy in the digital age Report of the Office of the United Nations High Commissioner for Human Rights, 2014. Retrieved January 09, 2015, from http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

Rahimi, B., The agonistic social media: cyberspace in the formation of dissent and consolidation of state power in postelection Iran. *The Communication Review*, 2011.

Reporters Without Borders [RSF], *Press Freedom Barometer 2014*, 2014.

Rhoads, C., & Fassihi, F., Iran Vows to Unplug Internet. *Wall Street Journal*, 2011.

RSF. (2014a). Enemies of the Internet. Retrieved February 15, 2015, from http://12mars.rsf.org/2014-en/#slide2

RSF. (2014b). *Press Freedom Barometer 2014*.

Scott-Railton, J., & Hardy, S., Malware Attacks Targeting Syrian ISIS Critics. *Citizen Lab*, 2014. Retrieved January 08, 2015, from https://citizenlab.org/2014/12/malware-attack-targeting-syrian-isis-critics/

Tanriverdi, H., Bürgerkrieg in Syrien: Das Internet als Kriegswaffe - Digital - Süddeutsche.de. *sueddeutsche.de*, 2015. Retrieved January 06, 2015, from http://www.sueddeutsche.de/digital/buergerkrieg-in-syrien-das-internet-wird-als-kriegswaffe-eingesetzt-1.2289887

Tikk, E., Global Cybersecurity–Thinking About the Niche for NATO. *SAIS Review*, *30*(2), 105–119, 2010.

Tufekci, Z., Algorithms in our Midst: Information, Power and Choice when Software is Everywhere. *Proceedings of the 18th ACM Conference on Computer …*, 2015.

Van Eeten, M. J., & Mueller, M., Where is the governance in Internet governance? *New Media & Society*, *15*(5), 720–736. doi:10.1177/1461444812462850, 2012.

Wagner, A. Ben, Digital Rights in Turkey, 2014. Retrieved January 09, 2015, from https://cihr.eu/digital-rights-in-turkey/

Watt, N., & Wintour, P., Facebook and Twitter have "social responsibility" to help fight terrorism, says David Cameron | World news | The Guardian. *The Guardian,* 2015. Retrieved March 05, 2015, from http://www.theguardian.com/world/2015/jan/16/cameron-interrupt-terrorists-cybersecurity-cyberattack-threat

Whitefield, M., Security concerns could cast a shadow on 2014 World Cup in Brazil | The Miami Herald, 2014. Retrieved January 09, 2015, from http://www.miamiherald.com/news/nation-world/world/americas/article1952843.html

Yadron, D., Obama Sides with Cameron in Encryption Fight - Digits - WSJ. *Wall Street Journal*, 2015. Retrieved February 12, 2015, from http://blogs.wsj.com/digits/2015/01/16/obama-sides-with-cameron-in-encryption-fight/

York, J. C., Policing Content in the Quasi-Public Sphere. Boston, MA: Open Net Initiative Bulletin. Berkman Center. Harvard University, 2010.

Zalnieriute, M., *ICANN's Corporate Responsibility to Respect Human Rights*. London, 2015.

Zalnieriute, M., & Schneider, T., *ICANN's procedures and policies in the light of human rights, fundamental freedoms and democratic values* (pp. 1–49). Strasbourg, 2014.

EUROPEAN PARLIAMENT

QA-04-15-288-EN-C (print)
QA-04-15-288-EN-N (pdf)

DIRECTORATE-GENERAL FOR EXTERNAL POLICIES

POLICY DEPARTMENT

Role

Policy departments are research units that provide specialised advice to committees, inter-parliamentary delegations and other parliamentary bodies.

Policy Areas

- Foreign Affairs
  - Human Rights
  - Security and Defence
- Development
- International Trade

Documents

Visit the European Parliament website: **http://www.europarl.europa.eu/studies**

PHOTO CREDIT: iStock International Inc.

ISBN 978-92-823-7025-4 (print)
ISBN 978-92-823-7024-7 (pdf)
doi:10.2861/676232 (print)
doi:10.2861/035360 (pdf)

Publications Office