
Council of Europe Conference of Ministers responsible for Media and Information Society

FREEDOM OF EXPRESSION AND DEMOCRACY IN THE DIGITAL AGE

OPPORTUNITIES, RIGHTS, RESPONSIBILITIES

Belgrade, 7-8 November 2013

Republic of Serbia
Ministry of Culture and Information

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

MCM(2013)008

# Internet freedom and the right to private life, protection of personal data and due process of law

**Report submitted by Access (AccessNow.org):**
**Raegan MacDonald, Jochai Ben-Avie, and Fabiola Carrion**

Website: https://www.accessnow.org/

E-mail: raegan@accessnow.org

# Table of contents

## Executive Summary

Internet freedom today can and must encompass a broader range of human rights beyond freedom of expression. These include, but are not limited to, the right to private life (Article 8), freedom of expression, which includes freedom of the media (Article 10), the freedom to assimilate and associate (Article 11), freedom of thought (Article 9), and the right to remedy (Article 13). These rights have been long established in several international instruments, including the International Covenant of Civil and Political Rights (ICCPR) and the European Convention on Human Rights and now need to be protected and realised more effectively in the digital environment.

The advances in, and the increasing use of communications technology have enabled surveillance at an unprecedented scale. The growing dependence on technology -- to connect us, conduct business and even manage critical domestic infrastructure -- amplifies the threat to human rights when users, businesses, and governments lose trust in these systems. When trust is broken, we risk not only undermining Internet freedom, but squandering the benefits of the digital environment for all people.

This report outlines the challenges associated with realising Internet freedom, with a particular focus on the right to private life, data protection, and due process of law, particularly in the context of this summer's revelations of mass surveillance. The report identifies elements for public policy responses and proposes lines of action that can be undertaken within the mandate of the Council of Europe. A parallel report addresses Internet freedom, with a focus on the rights to freedom of expression, freedom of association, and freedom of the media in Europe.

The Council of Europe has long played a role as a standard setter in the area of human rights, for Europe and around the world. The Council of Europe Committee of Ministers and Parliamentary Assembly have adopted important declarations, resolutions, and recommendations advancing and promoting Internet freedom. To respond to new challenges, to mitigate future human rights impacts, and to achieve its Internet freedom agenda, the Council of Europe should consider the following recommendations, which are elaborated in more detail in Section 2 of this report:

***Seizing the opportunity to make Convention 108 a global privacy standard***

Privacy is a key building block for democratic freedoms. The Council of Europe can play a defining role in restating and reinforcing international norms by effectively updating the Convention and working proactively for wide ratification.

***Strengthen oversight and implementation of the updated Convention***

To enhance implementation and strengthen oversight of compliance, each authority in the signatory countries should appoint a single point of contact dedicated to the Convention on the national level. This group of appointees can coordinate through periodic meetings and also play a key role in responding to emerging technological challenges by producing common guidance on specific issues.

***Tightening any remaining gaps in the Convention***

For the Convention to truly serve its role as a model for the protection of personal data, loopholes must be avoided, as the Convention will only be as strong as its weakest link. The Council of Europe Consultative Committee (T-PD), which has already worked diligently on the modernisation efforts, should ensure that key elements are not weakened in favour of what some states have called greater "interoperability" of data protection systems.

***Strengthening the role of Data Protection Authorities***

In order for data protection authorities to effectuate their mandates, their independence from the executive structure of member state governments is absolutely critical. While the Council of Europe has already recognised the importance of ensuring that data protection authorities have independence and adequate resources, Council of Europe members should ensure that proposals to integrate the additional protocol of the Convention into the updated version of Convention 108 are implemented. On a member state level, regulation should be implemented - or supported - to further strengthen the position of the relevant authorities.

***Adopting and Implementing the Principles on the Application of Human Rights to Communications Surveillance***

To address challenges facing the protection of user rights with regards to communications surveillance, the Principles on the Application of Human Rights to Communications Surveillance (crafted by civil society) are instructive. The Council of Europe, acting on both the regional and national levels, should play a leading role in promoting Internet Freedom through the adoption and implementation of these Principles.

Furthermore, the CoE's Human Rights Education for Legal Professionals Programme (HELP), which already undertakes globally significant work in this area, should integrate the Principles into future events, training, and other activities which help to develop common standards and further international cooperation in the application of human rights law to communications surveillance.

***Engaging in greater transparency***

As transparency is a key element to ensuring accountability of governments and corporations, the Council of Europe should strongly consider expanding its transparency agenda to include publicly available, annual reports on state surveillance practices. To provide greater accountability and verification, Council of Europe member states should urge companies to publish the same information.

***Re-establishing trust in the corporate sector***

It is important to build upon the work already put in motion by the Council of Europe, in particular through the CoE's drafting group on human rights and business (CDDH-CORP). The recent revelations regarding the nature and scale of mass surveillance have shown that more guidance, beyond what is already established in current frameworks

(e.g. UN Guiding Principles on Business and Human Rights), is needed. The CoE and its member states should take proactive steps to develop timely and sector and/or sub sector specific guidelines on how companies can uphold their responsibilities to respect human rights, particularly in regards to challenges to Internet freedom.

***Promoting Digital Literacy***

For states to uphold their positive obligations to protect human rights, citizens must be empowered to have greater control over their personal data, make informed choices about their online habits, and be more aware of the potential risks and how they may protect themselves. While the Council of Europe has already recognised the need to raise awareness in school environments concerning the rights of others in the exercise of freedom of expression, this action line can and should be broadened to encompass the wide range of rights that relate to Internet freedom, in particular privacy and data protection.

Furthermore, Council of Europe member states should promote the use of open source privacy enhancing tools and allocate specific funding streams towards the design, development, and deployment of these technologies.

***Ensuring greater protection for whistleblowers***

To promote and ensure that abuses of human rights and corruption are exposed, the Council of Europe and its member states should urgently establish greater protections for whistleblowers. The work of the European Committee on Legal Co-operation (CDCJ) is exemplary in this regard, and the (draft) recommendation on the protection of whistleblowers should be energetically supported by the Council of Europe and the individual member states.

## Introduction

Recent revelations of surveillance by various state intelligence agencies have provoked a strong response from international human rights authorities. United Nations High Commissioner for Human Rights Navi Pillay noted that these government practices "raise a number of important international human rights issues which need to be addressed."[1] In his most recent report, A/HRC/23/40, U.N. Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression Frank La Rue similarly stresses the need for due process and judicial oversight to guarantee these fundamental rights in the course of state surveillance.[2] Indeed, this summer's revelations of sweeping state surveillance demonstrate most clearly the need for an expanded Internet freedom agenda.

The explosion of digital communications content, "communications metadata,"[3] the falling cost of storing and mining large data sets by third-party services, the ability to combine and organise different datasets, and the increased sensitivity of the information available to be accessed make surveillance possible at an unprecedented scale, posing growing dangers to fundamental rights. As societies increasingly conduct the majority of communications through electronic means, the most personal and intimate details about a person's past, present, or future actions can be divulged.

This summer's reports detailing the scope of state surveillance programs have demonstrated that this is not some dystopian future, but rather today's reality. Every email, every phone call, every Facebook post, every bank transaction, literally every communication and activity on the Internet and telecommunications networks can and is potentially being surveilled by the U.S.' National Security Agency, its British counterpart, the GCHQ, as well as other government intelligence services. Indeed, as the Committee of Ministers has acknowledged in its 11 June 2013 Declaration on Risks to Fundamental Rights Stemming from Digital Tracking and other Surveillance Technologies, "These capabilities and practices can have a chilling effect on citizen participation in social, cultural and political life and, in the longer term, could have damaging effects on democracy."[4] This includes, more generally, the endangerment of the freedom to receive and impart information, as enshrined in Article 10 and Article 8 of the European Convention on Human Rights.

---

1 U.N. Office of the High Commissioner for Human Rights, "Mass surveillance: Pillay urges respect for right to privacy and protection of individuals revealing human rights violations," http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=13534&LangID=E

2 La Rue, Frank. Report of the Special Rapporteur on the Promotion and Protection of the right to freedom of opinion and expression, A/HR/23/40.

3 La Rue, Frank. Report of the Special Rapporteur on the Promotion and Protection of the right to freedom of opinion and expression, A/HR/23/40(establishes that communications data "includes personal information on individuals, their location and online activities, and logs and related information about the e-mails and messages they send or receive."), para 6. [hereinafter Frank La Rue A/HR/23/40 Report].

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

The Vienna Declaration and Programme of Action instructs that human rights are "universal, indivisible and interdependent and interrelated." The freedoms of expression and association cannot be fully exercised when the rights to privacy and due process are not adequately protected. The Council of Europe has acknowledged as much, in its Internet Governance Strategy stating, "The freedom, dignity and privacy of Internet users must be a central concern and priority for democracies, especially governments which rely upon and encourage the use of new technologies."[5] This and other aspects of the Council of Europe's Internet freedom agenda can be further developed to address the challenges to privacy and due process posed by modern day surveillance. So too must this agenda speak to the role of the private sector, especially in regards to data protection rules; after all, most of the information analysed by the NSA, GCHQ, and other intelligence agencies was initially collected by tech companies.

This report shall take stock of the challenges and threats to Internet freedom in Council of Europe Member States and shall analyse the roles and responsibilities of state and non-state actors in protecting it, with particular reference to:

> *The right to private life, including monitoring and surveillance of communications and activities of Internet users, compliance with the requirements of international law, notably the European Convention on Human Rights and the jurisprudence of the European Court of Human Rights;*
>
> *The right to privacy with regard to personal data, including collection and processing of personal data by state and non-state actors, safeguards and procedural guarantees (due process), compliance with international law notably Convention for the Protection of Individuals with Regards to Automatic Processing of Personal Data (ETS No.108 & ETS 181);*
>
> *Capacity building and digital literacy, including the need to ensure citizens are well informed on data collection and processing practices of state and non-state actors, and empowered to take control of their personal data.*

On this basis, the report shall identify elements for responses and desirable lines of action within the mandate of the Council of Europe to address threats to Internet freedom by States, in particular to ensure the enforceability of privacy protection rules, including engaging the business sector regarding compliance and accountability in respecting human rights on the Internet.

## Section 1: Challenges

### *1.1 Advances in technology enable surveillance at a scale previously unimaginable*

The surveillance programs revealed by former NSA contractor Edward Snowden, journalist Glenn Greenwald, and filmmaker Laura Poitras have shaken the world. In

5 Council of Europe's Internet Governance Strategy 2012-2015, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/internet%20Governance%20Strategy/Internet%20Governance%20Strategy%202012%20%202015.pdf, no.10

June of 2013, it was reported that the U.S. government was accessing in bulk, and on "an ongoing and daily basis,"[6] the metadata of telecommunications customers in the United States. Shortly after this revelation, nine Internet and technology companies were found to be providing to the U.S.' National Security Agency access to the content of their customers' data through a program code-named Prism.[7] A handful of related programs, such as XKeyScore which allows the U.S. government to access and search anyone's email content, online searches, social media activity, and metadata also came to light.[8] It has additionally become common knowledge that other major world powers like the U.S., United Kingdom, Canada, Australia, and New Zealand are also fully accessing and sharing communications data of their citizenry in an informal intelligence agreement called "Five Eyes."[9]

Furthermore, as reported by the Guardian, Great Britain's GCHQ is working hand-in-hand with the NSA to "directly" receive data from the undersea and terrestrial fibre optic cables that provide the backbone of the Internet's infrastructure. Through programs which catch data passing "upstream" like STELLAR WIND, FAIRVIEW, BLARNEY, OAKSTAR, LITHIUM, STORMBREW, and TEMPORA,[10] the NSA, GCHQ, and other intelligence services have the capabilities to gain access to *all* telephone and Internet traffic passing through the fibre optic cables that connect most of the world as well as roughly 75% of the U.S. domestic network.[11]

Our societies are becoming increasingly reliant upon communications technology: to connect with friends, loved ones, colleagues, to conduct business – indeed, a large portion of commerce has moved online – but also much of critical infrastructure in many countries, such as the electric power grid, can all be controlled and accessed online. These systems must be trustworthy. Yet, law enforcement, and more broadly, national security policies, have remained narrowly focused on surveillance. Such an approach has presented citizens with a Faustian trade-off between security and privacy, suggesting that one must be sacrificed in order to have more of the other. This is a false juxtaposition. As reports from the Guardian show, the NSA, GCHQ, and other intelligence agencies increasingly introduce new vulnerabilities into the Internet's architecture[12],

---

6The Guardian, "NSA collecting phone records of millions of Verizon customers daily," http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

7The Guardian, "NSA Prism program taps into user data of Apple, Google and others," http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

8The Guardian, "XKeyscore: NSA tool collects 'nearly everything a user does on the ," http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

9 The Guardian, "NSA leaks: US and Britain team up on mass surveillance," http://www.theguardian.com/world/2013/jun/22/nsa-leaks-britain-us-surveillance

10The Guardian, "GHCQ taps fibre-optic cables for secret access to world's communications," http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

11The Wall Street Journal, "New Details Show Broader NSA Surveillance Reach," http://online.wsj.com/article/SB10001424127887324108204579022874091732470.html
12 The Guardian, "Revealed: how US and UK spy agencies defeat internet privacy and security," http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

which not only poses significant challenges for the protection of privacy of users worldwide, but also threatens the integrity and security of this globally shared resource.

Given that the channels upon which we communicate are primarily owned and operated by corporate actors, tech companies are necessarily implicated in the realization of Internet freedom. The U.N. Guiding Principles on Business and Human Rights make clear that companies have the responsibility to *respect* human rights, which is especially true as they design, develop, and implement technologies that facilitate surveillance.

### *1.2 Surveillance conducted through circumvention of due process of law*

Law enforcement and state security agencies have demonstrated an increased interest in getting access to the myriad data that is produced, collected, and stored as a result of the ubiquity of communications technology. The growing prevalence of cloud computing (e.g. where data is stored on the Internet by a third party service instead of on a personal computer)[13] adds further complexity in terms of enforcing national and regional human rights-protecting regulation, as data is increasingly stored in sometimes conflicting jurisdictions. This creates a challenge to ensuring adequate protection for user privacy, where the privacy standards in the user's region or country of origin may conflict with where that data is stored, processed, or travels through.

The Council of Europe's Commissioner for Human Rights Nils Muižnieks also stated that, "Proportionality and judicial oversight appear as two particularly key principles that should be systematically applied when looking at issues such as restricting access to Internet content or carrying out surveillance on the Internet activities of specific individuals."[14] However, as articulated in his A/HRC/23/40 report, Special Rapporteur La Rue cautioned that this dynamic represents a challenge for due process as "access to communications data can be obtained in many States without independent authorisation and with limited oversight."[15]

13 See EDRi Booklet writte by members and observers, "An Introduction to Data Protection" (Spring 2013), http://www.edri.org/files/paper06_datap.pdf

14 Comment of the Council of Europe Commissioner for Human Rights, "Press freedom in the digital age: New Threats, New Challenges, " http://humanrightscomment.org/2013/05/03/press-freedom/

15 Frank La Rue A/HR/23/40 Report, para. 17

Laws regulating the ability of States to conduct surveillance, particularly obligations of necessity, proportionality, and legitimacy are either inadequate to the task or simply do not exist. This creates an environment which is ripe for abuse and puts the rule of law under strain.[16]

### *1.3 Lack of clarification on the right to privacy inhibits its protection*

While the right to privacy has been enshrined in nearly all international, regional, and national legal frameworks, in practice, these documents do not contain operational level guidance on how this right should be protected.

La Rue suggests that States may benefit from a more nuanced articulation of what privacy means and how current technologies can interfere with this right. He defines privacy as "the presumption that individuals should have an area of autonomous development, interaction and liberty, a "private sphere" with or without interaction with others, free from State intervention and from excessive unsolicited intervention by other uninvited individuals."[17]

Furthermore, according to Article 8 of the European Convention on Human Rights, any interference with the right to privacy must occur in accordance with law, serve a legitimate goal (set out in Art 8(2)), and be necessary in a democratic society. Given the flagrant intrusions into private life on national,[18] regional,[19] and international levels,[20] it appears that there is insufficient guidance to States in making these determinations or protecting this balance.

In response to these challenges, and intended to serve as a guide for states in assessing the compliance of communications surveillance practices with international law and human rights norms, a group of civil society organisations and legal experts have crafted the "International Principles on the Application of Human Rights to Communications Surveillance".[21] The Principles are instructive here and are worth quoting at length:

> Traditionally, the invasiveness of communications surveillance has been evaluated on the basis of artificial and formalistic categories. Existing legal frameworks distinguish between "content" or "non-content," "subscriber

16 See Frank La Rue A/HR/23/40 Report, para. 3 & 17.

17 Frank La Rue A/HR/23/40 Report

18 Ton Siedsma (Bits of Freedom), https://www.bof.nl/2013/05/02/dutch-hacking-proposal-puts-citizens-at-risk/ 2 May, 2013

19 Access, Commonwealth of Surveillance States: on the Export and Resale of Russian Surveillance Technology to Post-Soviet Central Asia, https://www.accessnow.org/page/-/docs/Commonwealth_of_Surveillance_States_ENG_1.pdf

20 The Washington Post, "Agreements with private companies protect U.S. access to cables' data for surveillance," http://www.washingtonpost.com/business/technology/agreements-with-private-companies-protect-us-access-to-cables-data-for-surveillance/2013/07/06/aa5d017a-df77-11e2-b2d4-ea6d8f477a01_story.html?Post+generic=%3Ftid%3Dsm_twitter_washingtonpost

21 International Principles on the Application of Human Rights to Communications Surveillance, https://en.necessaryandproportionate.org/text (hereinafter "13 International Principles")

information" or "metadata," stored data or in transit data, data held in the home or in the possession of a third party service provider.[22] However, these distinctions are no longer appropriate for measuring the degree of the intrusion that communications surveillance makes into individuals' private lives and associations. While it has long been agreed that communications content deserves significant protection in law because of its capability to reveal sensitive information, it is now clear that other information arising from communications – metadata and other forms of non-content data – may reveal even more about an individual than the content itself, and thus deserves equivalent protection. Today, each of these types of information might, taken alone or analysed collectively, reveal a person's identity, behaviour, associations, physical or medical conditions, race, colour, sexual orientation, national origins, or viewpoints; or enable the mapping of the person's location, movements or interactions over time,[23] or of all people in a given location, including around a public demonstration or other political event. As a result, all information that includes, reflects, arises from or is about a person's communications and that is not readily available and easily accessible to the general public, should be considered to be "protected information", and should accordingly be given the highest protection in law.

In evaluating the invasiveness of State communications surveillance, it is necessary to consider both the potential of the surveillance to reveal protected information, as well as the purpose for which the information is sought by the State. Communications surveillance that will likely lead to the revelation of protected information that may place a person at risk of investigation, discrimination or violation of human rights will constitute a serious infringement on an individual's right to privacy, and will also undermine the enjoyment of other fundamental rights, including the right to free expression, association, and political participation. This is because these rights require people to be able to communicate free from the chilling effect of government surveillance. A determination of both the character and potential uses of the information sought will thus be necessary in each specific case.

### *1.4 Lack of transparency around data collection*

Transparency in government activity is a critical precondition for the accountability of States and for the free, full, and safe participation in society of all people. For too long, surveillance has occurred in the shadows - including little to no voluntary disclosure of

22 "People disclose the phone numbers that they dial or text to their cellular providers, the URLS that they visit and the e-mail addresses with which they correspond to their Internet service providers, and the books, groceries and medications they purchase to online retailers….. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection." United States v. Jones, 565 U.S. ___, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

23 "Short-term monitoring of a person's movements on public streets accords with expectations of privacy" but "the use of longer term GPS monitoring in investigations of most offences impinges on expectations of privacy." United States v. Jones, 565 U.S. __, 132 S. Ct. 945, 964 (2012) (Alito, J. concurring).

what data are being collected, for what purposes, and with whom they are being shared. Indeed, this summer's revelations have shown that a lack of transparency has contributed to systemic abuse of human rights.

As Louis Brandeis said, "sunlight is the best disinfectant" and greater transparency around government surveillance activities and requests for user data, whether for national security or in the furtherance of traditional criminal law enforcement, is a critical first step. In this regard, many of the companies implicated in the NSA PRISM program, including Google, Facebook, Yahoo!, and Microsoft, have released transparency reports and are fighting in the Foreign Intelligence Surveillance Court to be released from the gag orders that prevent them from reporting more granular details about their involvement with state surveillance.[24] These and other companies have joined with a number of civil society groups, investors, and trade associations in the WeNeedToKnow Coalition [25] to also push the US Congress and the Obama Administration to allow companies to report on the specific number of requests they receive, under which statutes, the specific number of users/devices affected, and the specific authorities making requests. The Coalition further asks for the government to release the same information, which would provide credible, two-way verification and accountability.

While the Office of the US Director of National Intelligence has said the US government will release a transparency report, including requests authorized by the Foreign Intelligence Surveillance Act and the Patriot Act, it falls far short of this standard.[26] Furthermore, currently, not a single member of the Council of Europe releases a transparency report that includes requests made pursuant to national security-related investigations.

It's worth noting that several countries release reports detailing requests made in the furtherance of traditional criminal investigations with seemingly no adverse effects.[27] And while a transparent wrong is still a wrong, taking concrete steps to inform citizens about how States are conducting surveillance allows for individuals, civil society organizations, data protection authorities, and national human rights institutions to hold governments and companies accountable.

In addition to providing greater accountability, detailed transparency reports allow for a more informed public debate over state surveillance and necessary legal reforms. Credible reports similarly can aid data protection authorities and national human rights institutions in better understanding the scope, nature, and application of surveillance

24 Politico, "Yahoo, Facebook file suits on surveillance orders,"http://www.politico.com/story/2013/09/yahoo-facebook-surveillance-orders-96506.html

25 Access, "We need to know: companies, civil society call for transparency on surveillance," https://www.accessnow.org/blog/2013/07/18/tech-companies-and-civil-society-join-call-on-the-us-government-to-is

26 Access, "Obama Administration continues to thwart meaningful transparency on NSA surveillance, https://www.accessnow.org/blog/2013/08/30/obama-administration-continues-to-thwart-meaningful-transparency-on-nsa-sur

27 See 2012 Annual Report of the Interception of Communications Commissioner, http://www.iocco-uk.info/docs/2012%20Annual%20Report%20of%20the%20Interception%20of%20Communications%20Commissioner%20WEB.pdf

practices, so they can more efficiently assign resources to meet challenges to privacy and data protection, thereby more efficaciously fulfilling their mandates. Finally, by providing details of abuses, transparency reports allow users to seek redress for harms, in line with Article 13 of the European Convention on Human Rights.

### *1.5 Corporate infringements of human rights*

A staggering majority of data acquired and analysed in the course of surveillance isn't actually collected by States themselves, but rather by companies that users, businesses, and even governments are generating in record amounts. And it is big business indeed. Personal data is often labeled as the "currency" of the digital age. The mining and harvesting of personal data has become a multi-billion dollar business. In Europe alone, the value of European citizens' data in 2011 was 315 billion Euros. It's estimated to reach near 1 trillion annually by 2020.[28]

But data isn't just "currency," as these collected pieces of information relate to individuals' private lives. Indeed, the European Court of Human Rights has acknowledged that the mere processing of personal data could represent an interference with the right to private life.[29] As recognised by the Council of Europe, the protection of personal data is a basic right; according to Convention 108 it is afforded to "every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection")."

Given that data collected by companies are the fuel of the surveillance machine, the roles and responsibilities of the private sector merit special attention. The U.N. Guiding Principles on Business and Human Rights oblige corporate actors to respect human rights and remedy abuses when they occur. To complement the high-level guidance of the Principles, the European Commission, in cooperation with industry, civil society and consumer rights stakeholders, has recently produced the "ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights",[30] a manual on how companies can apply these obligations. States should encourage the development of guidance for companies operating both within and outside of their borders to ensure comprehensive protection of the rights of their citizens.

The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108") provides a strong baseline for data protection, of which the sum of the principles could serve to reduce the privacy risks associated with electronic communications surveillance. For state and non-state actors collecting data, this would mean, for instance, collecting less data (data minimisation), ensuring that

28 Viviane Redding, "Data protection reform: restoring trust and building the digital single market European Commission," SPEECH/13/720, 17.9.2013, http://europa.eu/rapid/press-release_SPEECH-13-720_en.htm

29 See "Case law of the European Court of Human Rights concerning the protection of personal data", (30 January 2013) http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/DP%202013%20Case%20Law_Eng%20%28final%29.pdf

30 European Commission, ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights, http://ec.europa.eu/enterprise/policies/sustainable-business/files/csr-sme/csr-ict-hr-business_en.pdf

personal data is collected and stored for strictly defined purposes, and not used in a way that is incompatible with those purposes (Article 5), and applying appropriate security measures to data that is stored (Article 7). In practice this could mean the implementation of privacy by design, as included in the EU's proposed Data Protection Regulation and Article 8bis (3) in the modernisation proposals of the Convention.[31]

For users, having control over personal data is paramount as it empowers citizens to make informed decisions about who may have access to their data and with whom they share them with. Article 8 of Convention 108 is instructive in this regard as it includes the right to access, deletion, or rectification. States should establish national level protections with strong compliance mechanisms built in. The EU's proposed Data Protection Regulation is also instructional in this regard, as it seeks to give citizens control over their data, harmonise the rules, and increase enforcement powers in the EU.[32] However, the final value of the proposal will be determined by the outcome of the process which is currently underway and which has been subject to unprecedented lobby efforts by third countries and companies, many of which are implicated in the PRISM scandal.[33]

As the privacy of communications is essential for the freedoms of expression and association, companies can play a role in upholding their duty to respect human rights by supporting the exercise of anonymous speech. In the course of roughly a decade and a half, the Internet has become an invaluable and depended resource to find reliable, sometimes private information, as well as a forum for discussion and expression. There are a range of reasons individuals may need to communicate anonymously or pseudonymously, whether an LGBT teen, a survivor of domestic violence, a human rights activists targeted by their government as a dissident, a whistleblower or journalist fighting to expose an abuse of power, or simply someone that wishes to keep their online activities private. Just as one feels more comfortable saying certain things in the privacy of one's home rather than the public square, so too does online surveillance have a chilling effect on freedom of expression on the web. Ensuring the ability to participate online anonymously, and more generally the privacy of communications, is critical to ensuring that individuals are able impart and receive information without fear or reprisal or embarrassment.

The Council of Europe has already recognised the importance of anonymity to enhance free expression and the free flow of ideas in the Declaration on Freedom of Communication on the Internet (2003),[34] and has identified in its Internet Governance Strategy 2012-2015 that a review of these standards is in order. This review must pay

31 See: T-PD(2012)04rev2en (16 October 2012), http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD_2012_04_rev2_En.pdf

32 See EDRi's "Key Issues for the Data Protection Regulation" (Spring 2013) http://protectmydata.eu/briefguide/key-issues/

33 See EDRi and Access, "Lobbying Against the Data Protection Regulation (Spring 2013) http://www.edri.org/files/eudatap-03.pdf and from the EDRi blog, "US lobbying against the data protection reform intensifies (17 January 2013) http://www.edri.org/us-eudatap

34 Committee of Ministers Declaration on freedom of communication on the Internet, https://wcd.coe.int/ViewDoc.jsp?id=37031, 28.05.2003

particular note to the challenges to anonymity and pseudonymity on the web that arise when Internet and telecommunication traffic is unencrypted, which will be discussed in the next section.

### *1.6 Unencrypted Internet traffic and increasing pressure on private companies to build security vulnerabilities into products and services*

As data packets flow over the Internet from users' computers to website servers they pass through around fifteen intermediary routers, typically traversing the terrestrial and undersea fibre optic cables that make up the backbone of the Internet.[35] It has already been discussed that reports from the Guardian reveal that the NSA and GCHQ are tapping these fibre optic cables, allowing them to intercept and collect nearly all communications, generally without ever having to serve a company with a specific court order.[36] These intelligence agencies are able to analyse these data freely because most Internet traffic is unencrypted. When websites encrypt their users' traffic, intelligence agencies and law enforcement must instead go to these websites directly to acquire user data, involving significantly more procedural safeguards. While some companies like Blackberry have been forced to turn over their master encryption keys to various governments,[37] other companies such as Microsoft are proactively and seemingly without compulsion handing over their encryption keys to services like Outlook and Skydrive,[38] the company's cloud storage service.

At the same time that the NSA is engaging in surveillance, it is also charged with protecting cybersecurity. To this end, the NSA works hand-in-hand with tech companies, supposedly to help them secure their networks, but it appears that they have also been building in backdoors to be exploited later.[39] But these vulnerabilities aren't just accessible to the NSA, third parties including other governments and malicious hackers can make use of them too, leaving all users less secure.[40]

The US achieves a similar feat through legislation as well. The Communications Assistance for Law Enforcement Act (CALEA) requires all telecommunications companies to design their networks to make wiretapping easier. However, it explicitly does not force companies handling Internet traffic (including VOIP providers) to build in such backdoors, something the US' law enforcement and national security establishment is currently trying to change.

---

35 University of Washington - Computer Science and Engineering, Reverse Tracerout Network Diagnostic Utility, http://revtr.cs.washington.edu/FAQ.html#how

36 See footnote 10

37 The Economic Times, "Black Berry maker Research in Motion agrees to hand over its encryption keys to India," http://articles.economictimes.indiatimes.com/2012-08-02/news/33001399_1_blackberry-enterprise-encryption-keys-corporate-emails

38 The Guardian, "Microsoft handed the NSA access to encrypted messages," http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data

39 The New York Times, "N.S.A. able to foil basic safeguards of privacy on web," http://www.nytimes.com/2013/09/06/us/nsa-foils-much--encryption.html?pagewanted=all&_r=0

40 Access, "You wouldn't leave your backdoor unlocked: the danger of intentional vulnerabilities," https://www.accessnow.org/blog/2013/09/20/you-wouldnt-leave-your-backdoor-unlocked-the-danger-of-intentional-vulnerab

The last time US law enforcement and national security agencies sought to build in a backdoor into all communications handling encrypted traffic, the "Clipper Chip" initiative of the 1990s, the classified encryption algorithm on the chip ultimately proved to be insecure and the Clipper protocol easy to circumvent. Backdoors at their most fundamental level introduce a hole into secure communications where none existed previously, so whether they are purely algorithmic or protocol-based, their exploitation only takes a dedicated attacker and time.[41] Enforcing the use of a defective product highlights the contradiction of backdoors: they give users an insecure product in the name of the user's security. The public rejected that contradiction twenty years ago, and it's a problem we must still contend with today.

### *1.7 Justification for surveillance laws increased at the expense of necessity, proportionality, and legitimate aim.*

La Rue has noted in his most recent report that, "changes in technology have been paralleled by changes in attitudes towards communications surveillance." In the United States, for instance, such surveillance (e.g. wiretapping) was carried out on a restricted basis and only "reluctantly sanctioned" by courts. He continues, "over time, however, States have expanded their powers to conduct surveillance, lowering the threshold and increasing the justifications for such surveillance."[42]

The worldwide adoption of communications data retention is notable in this regard. For instance, the Data Retention Directive, adopted by the European Union in 2006, mandates that all telecommunications data – including from mobile and landline phones, fax, and email – are indiscriminately collected and retained for six months up to two years. This mass retention of the activities of citizens, outside of the context of any criminal investigation, poses significant challenges to the very foundations of the rule of law and international human rights, including Article 8 of the European Convention on Human Rights.

In several Member States, including Romania, Sweden, the Czech Republic, and Germany, the laws transposing this Directive were successfully challenged on the grounds of constitutionality.[43] Furthermore, the European Commission has never been able to credibly demonstrate the necessity and proportionality of blanket data retention.[44]

The European Court of Human Rights has weighed in as well, with a number of rulings concluding that the surveillance of traffic data violates Article 8 of the Convention;[45] that the retention of records on past activities constitutes an interference with the right

41 Bruce Schneier, "The problems with CALEA II" (4 June 2013), https://www.schneier.com/blog/archives/2013/06/the_problems_wi_3.html

42 Frank La Rue A/HR/23/40 Report, para. 16.
43 Internet Policy Review, EU Data Retention Directive finally before European Court of Justice, http://policyreview.info/articles/news/eu-data-retention-directive-finally-european-court-justice/162

44 Freedom Not Fear, Internal memo on EU communications data retention directive leaked (26 Jan 2012), http://www.vorratsdatenspeicherung.de/content/view/520/55/lang,en/

45 Amann v. Switzerland, ECtHR, Application No. 27798/95, 16.2.2000

to private life;[46] that surveillance is "unlawful" if it is indiscriminate and lacks a specific legal regime;[47] and finally, that surveillance can only be considered lawful when effective safeguards have been established that ensure minimum infringement of rights and when all other alternative means have been exhausted.[48]

To this last point, alternative, more proportionate means of surveillance, such as data preservation, exist which could prove more effective and less harmful to human rights. Data preservation, or "data freeze," would entail, for instance, judicial authorisation for preservation, on a case-by-case basis, where the target is reasonably believed to be engaged in criminal activities or legitimately under a criminal investigation.[49]

Research on how surveillance, and data retention specifically, affects societies leaves something to be desired and is often overlooked in most impact assessments in the passage of such laws. The fundamental issue, however, is that when citizens are under surveillance they change their behaviour; they are less likely to feel comfortable expressing themselves and therefore self-censor, or refrain from using certain channels of communication. This chilling effect isn't just speculation. A study conducted in Germany after the transposition of the Data Retention Directive in 2008 revealed that 11% of respondents had already abstained from using the phone, email or mobile on certain occasions. Furthermore, 52% said that they probably would not use telecommunication for confidential purposes, "contacts like drug counsellors, psychotherapists or marriage counsellors" because of data retention.[50]

The Directive is currently being challenged in the European Court of Justice on the grounds of potential violation of the European Charter of Fundamental Rights.[51] It is unclear when the ECJ will release its ruling and what effect this will have on mandatory data retention in the European Union.

### *1.8 Need for greater protection of sources and whistleblowers*

The systematic undermining of the security and privacy of communications means that these channels are no longer trustworthy, which has devastating effects on Internet freedom. In particular, a core value necessary for the realization of the freedom of the media -- the protection of journalistic sources, both online and offline -- is at great risk. Indeed, the Parliamentary Assembly has acknowledged that, "the protection of

46 Rotaru v. Romania, ECtHR, Application No. 28341/95, 4.5.2000

47 See Kruslin v. France, ECtHR, Application No. 11801/85, 24.4.1990, Amann v. Switzerland, ECtHR, Application No. 27798/95, 16.2.2000; Kopp v. Switzerland, ECtHR, Application No. 13/1997/797/1000, 25.03.1998

48 See Privacy International, Briefing for Members of the European Parliament on data retention, Chapter II (26 Sep 2006), https://www.privacyinternational.org/reports/briefing-for-members-of-the-european-parliament-on-data-retention/invasive-and-illegal

49 See Open Rights Group, "Chapter Five Part I,"https://www.openrightsgroup.org/ourwork/reports/digital-surveillance/chapter-five-part-i; See also Caspar Bowden, "Submission to the Joint Committee on the draft Communications Data Bill", 23.8.2012

50 "Data Retention Effectively Changes the Behavior of Citizens in Germany" www.kreativrauschen.com/blog/2008/06/04/data-retention-effectively-changes-the-behavior-of-citizens-in-germany/, 4.06.2008

51Internet Policy Review, EU Data Retention Directive finally before European Court of Justice, http://policyreview.info/articles/news/eu-data-retention-directive-finally-european-court-justice/162

journalists' sources of information is a basic condition for both the full exercise of journalistic work and the right of the public to be informed on matters of public concern, as expressed by the European Court of Human Rights in its case law under Article 10 of the Convention."[52]

In the aftermath of the surveillance revelations, it has become clear that that unencrypted messages sent over the Internet are highly susceptible to interception by nearly any and every intelligence service in the world.[53] Furthermore, that the U.S. government "is willing and able to use telephone and Internet records to pursue sources who leak secrets to the media, and to do so by targeting reporters, if necessary."[54]

New York Times reporter James Risen said in an interview that, "the government's surveillance of both reporters and potential sources has made it much more difficult to do investigative reporting." He continues, "it's had a chilling effect on people in the government who are now afraid to talk to reporters."[55]

The protection of whistleblowers is intimately related to that of source protection, and the Council of Europe has already made substantial progress in this area, in particular through the European Committee on Legal Co-operation (CDCJ), whose draft recommendation on the protection of whistleblowers will be examined for adoption in the next Plenary meeting, and if adopted, passed to the Committee of Ministers in early 2014.[56]. To reiterate the Parliamentary Assembly's Resolution 1729 (2010) on the Protection of Whistleblowers, *"the importance of whistle-blowers – concerned individuals who sound an alarm in order to stop wrongdoings that place fellow human beings at risk – as their actions provide an opportunity to strengthen accountability and bolster the fight against corruption and mismanagement, both in the public and private sectors."* PACE calls on states to ensure that any "whistle-blowing legislation should focus on providing a safe alternative to silence", and the ability to guarantee the confidentiality of communications is crucial in this regard.

Despite this acknowledgement, a culture of intimidation prevails around the world. While Snowden, Greenwald, Poitras, and others have continued to publish critical information exposing the abuses of state surveillance, the harassment that they, their employers, friends, and family have faced is likely to have a significant chilling effect on other sources and whistleblowers that would speak out about abuses of human rights.[57] Moreover, in an age of pervasive surveillance, how much confidentiality can a journalist these days actually promise a source.

---

52 Parliamentary Assembly, Recommendation 1950 (2011) "The protection of journalists' sources" http://assembly.coe.int/Main.asp?link=/Documents/AdoptedText/ta11/EREC1950.htm

53Nieman Reports, "How to Keep Sources Secure from Surveillance"? 14.8.2013 http://www.nieman.harvard.edu/reports/watchdogarticle/100021/How-to-Keep-Sources-Secure-from-Surveillance.aspx,

54 Ibid.

55 Ibid.

56 CDCJ(2013) Misc7 final, http://www.coe.int/t/dghl/standardsetting/cdcj/2013/CDCJ%282013%29Misc7E.pdf

57 The Guardian, "David Miranda, schedule 7 and the danger that all reporters now face," http://www.theguardian.com/commentisfree/2013/aug/19/david-miranda-schedule7-danger-reporters

## Section 2: Recommendations

The Council of Europe Committee of Ministers and Parliamentary Assembly have passed a number of declarations, resolutions, and recommendations important for advancing and promoting Internet freedom. To respond to these challenges, mitigate future human rights impacts, and achieve its Internet freedom agenda, the Council of Europe should consider the following:

### *2.1 Seizing the opportunity to make Convention 108 a global privacy standard*

The Council of Europe has recognised that privacy and personal data are indispensable on the Internet[58] and should be a priority of Member States. The Convention, the first instrument of its kind, signed in 1981 and now ratified by 46 countries, has served as a solid baseline for the protection of personal data in the digital environment. The decision to seize the opportunity of accession to non-Council of Europe members through more dynamic and open approaches is also a welcome step, as the need to develop harmonised international standards for the protection of personal data has never been more pronounced. A few recommendations moving forward:

#### *2.1.1 Strengthen oversight and implementation of the updated Convention*

Each authority in the signatory countries should appoint a single point of contact dedicated to oversight and implementation of the Convention on the national level. These individuals should collectively meet periodically, and can play a more "hands on" role by producing common guidance on specific challenges and issues (e.g. big data and "smart" data). This task group should also meet periodically with a range of stakeholders, such as from academia, civil society, consumer protection groups, technologists, and industry.

#### *2.1.2 Tightening any remaining gaps in the Convention*

In order for the modernised Convention to serve its role as a model for the protection of personal data, loopholes must be avoided, as the Convention will only be as strong as its weakest link. The Council of Europe Committee of Ministers' Declaration on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies speaks to this point, when it "encourages member States to bear these risks in mind in their bilateral discussions with third countries". The Council of Europe Consultative Committee (T-PD) should therefore ensure that key elements of the Convention -- for instance that the threshold for transfer to third countries – are not weakened in favour of what some States have called greater "interoperability" of data protection systems.[59] To ensure maximum harmonisation and avoid loopholes, the text should [at least] remain consistent with existing instruments, including the EU's Data Protection Directive and the proposed Regulation.

---

58 See Council of Europe's Internet Governance Strategy 2012-2015, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/%20Governance%20Strategy/%20Governance%20Strategy%202012%20-%202015.pdf, no.10

59 Greenleaf, Graham, 'Modernising' Data Protection Convention 108: A Safe Basis for a Global Privacy Treaty? (May 8, 2013). (2013) Computer Law & Security Review, Vol 29, Issue 4; UNSW Law Research Paper No. 2013-33. Available at SSRN: http://ssrn.com/abstract=2262296

### *2.2 Strengthening the role of Data Protection Authorities*

In line with the proposals to integrate the additional protocol of the Convention into the updated version of 108,[60] and in recognition of the Declaration on Risks to Fundamental Rights Stemming from Digital Tracking and other Surveillance Technologies, it is critical to ensure the independence of the relevant authorities and ensure that they are adequately resourced to meet the challenges outlined in this paper. In particular, data protection authorities must operate outside of the executive structure of Member State governments, and therefore Article 12bis(4) in the modernisation proposals should be strongly supported. Furthermore, national-level regulation should be implemented - or supported - to further strengthen the position of the relevant authorities in enforcing their mandates, particularly in regards to administrative sanctions (as in Article 12bis 2(c)).

### *2.3 Adopting and Implementing the International Principles on the Application of Human Rights to Communications Surveillance*

The civil society-crafted International Principles on the Application of Human Rights to Communications Surveillance" ("The Principles") are currently endorsed by 280 organisations worldwide. The Principles draw from myriad international human rights treaties that establish the right to privacy, and cites regional human rights jurisprudence like the European Court on Human Rights.[61] The Council of Europe, acting on both the regional and national levels, should play a leading role in promoting Internet Freedom through the adoption, compliance, and implementation of The Principles.

The Council of Europe's Human Rights Education for Legal Professionals Programme (HELP) already does globally leading work in educating and alerting legal professionals to emerging challenges in this area. HELP should integrate the Principles into future convenings, trainings, and other activities which will help to develop common standards and further needed international cooperation in the application of human rights law to communications surveillance.

### *2.4 Engaging in greater transparency*

Recalling the commitments made in the Council of Europe's Convention on Access to Official Documents (CETS No. 205), furthering the commitments to open governance that several CoE Member States have made as members of the Open Government Partnership,[62] and based on the challenges explored throughout this paper with regards to the secrecy of communications surveillance and its corrosive effect on democratic principles, the Council of Europe should expand the transparency agenda to include publicly available, annual reports on state surveillance practices. These reports should include the specific number of requests, under which statutes, the specific number of

60 See Article 12bis on supervisory authorities, T-PD(2012)04rev2, http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD_2012_04_rev2_En.pdf

61 13 International Principles

62 Open Government Partnership, Open Government Declaration, http://www.opengovpartnership.org/open-government-declaration

users and devices affected, and the specific authorities making requests. The Parliamentary Assembly's resolution on National Security and Access to information[63] is instructive in this regard, and its call to member states to sign and ratify the CoE Convention on Access to Official Documents and in due course, further improve the convention to be more aligned with the Global Principles on National Security and the Right to Information, and/or related instruments, such as the International Principles on the Application of Human Rights to Communications Surveillance (see Section 2.3). To provide greater accountability and verification, Council of Europe Member States should compel companies to publish the same information.

### *2.5 Re-establishing trust in the corporate sector*

The Council of Europe has already made substantial progress in the area of business and human rights, notably through the 2008 "Human Rights Guidelines for Internet Service Providers",[64] written in collaboration with the Association of European ISPs (EuroISPA). However, in light of the specific challenges outlined in this paper, it is clear that more guidance, beyond what is already established in this and the U.N. Guiding Principles on Business and Human Rights, is needed.

The Council of Europe and its members should continue to take proactive steps to develop timely and sector and/or sub-sector specific guidelines on how companies can uphold their responsibilities to respect human rights.[65] In particular, the Council of Europe's Drafting Group on Human Rights and Business (CDDH-CORP)[66] should include guidance on challenges to Internet freedom.

On the national level, Member States should also seek to address the challenges outlined in this paper as they complete their National Action Plans implementing the U.N. Guiding Principles on Business and Human Rights.[67]

### *2.6 Promoting Digital Literacy*

The Council of Europe has already recognised in its Internet Governance Strategy the need to "raise awareness in school environments concerning the rights of others in the exercise of freedom of expression using online social media and other web-based applications."[68] This action line can and should be broadened to encompass the wide

63 Resolution 1954 (2013) Provisional version,
http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=20190&lang=en
64 Council of Europe, Human Rights Guidelines for Internet Service Providers,
http://www.coe.int/t/dghl/standardsetting/media/Doc/H-Inf(2008)009_en.pdf

65 European Commission, ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights,
http://ec.europa.eu/enterprise/policies/sustainable-business/files/csr-sme/csr-ict-hr-business_en.pdf, p. 9

66 Council of Europe, Corporate social responsibility in the field of human rights,
http://www.coe.int/t/dghl/standardsetting/hrpolicy/other_committees/hr_and_business/default_EN.asp

67 Institute for Human Rights and Business, "UK government prepares to launch National Action Plan on Business and Human Rights - Now the real work begins, " http://ihrb.org/commentary/staff/national-action-plan-on-business-and-human-rights.html

68 Council of Europe's Internet Governance Strategy 2012-2015, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/%20Governance%20Strategy/%20Governance%20Strategy%202012%20-%202015.pdf, Section V (h)

range of rights that relate to Internet freedom, in particular privacy and data protection. Education is needed which would empower students to exercise greater control over their personal data, make informed choices about their online habits, and be more aware of the potential risks and how they may protect themselves.

In furtherance of this last point, the Council of Europe Member States should promote the use of open source privacy enhancing tools and allocate specific funding streams as part of their Internet freedom budgets to the design, development, and deployment of these technologies. For example, the Swedish International Development Cooperation Agency funds the development of the Tor Project.[69]

### *2.7 Ensuring greater protections for whistleblowers*

The Parliamentary Assembly, in its Motion for a Resolution on Massive Eavesdropping in Europe has called on all Member States of the Council of Europe to, "Improve the protection against all forms of retaliation against bona fide whistle-blowers disclosing wrongdoings in the public interest."[70] To this end, the Council of Europe and its Member States should urgently establish greater protections for whistleblowers in order to limit any chilling effects on individuals in the future who would disclose abuses of human rights. As previously mentioned in this paper, the work of the CDCJ is exemplary in this regard, and the (draft) recommendation on the protection of whistleblowers[71] should be energetically supported by the CoE and the individual member states. Indeed, it is imperative that Member States create a safe and enabling environment for whistleblowers to come forward, as without these courageous individuals human rights abuses may often go unexposed. Whistleblowers shedding light on government abuses in particular frequently have to live out the rest of their lives in fear of reprisals and retribution, which highlights the important need for strong and open asylum policies.

The UN Human Rights Committee, the body charged with providing official interpretations of the International Covenant on Civil and Political Rights (ICCPR) in its General Comment No. 31[72] notes that, "the enjoyment of Covenant rights is not limited to citizens of State Parties, but must also be available to all individuals, regardless of nationality or statelessness, such as asylum seekers, refugees…" (para. 10). Member States should review their current asylum policies and ensure that they are in line with strong international standards such as that of General Comment 31. Indeed, in this regard, it is worth noting the difficulties that Snowden has encountered in his effort to seek asylum.[73]

---

69 See Tor Sponsors, https://www.torproject.org/about/sponsors.html.en

70 Parliamentary Assembly, Motion for a Resolution Motion for a resolution, Doc. 13288, 6 August 2013, "Massive eavesdropping in Europe", http://assembly.coe.int/ASP/XRef/X2H-DW-XSL.asp?fileid=20050&lang=EN

71 CDCJ(2013) Misc7 final, http://www.coe.int/t/dghl/standardsetting/cdcj/2013/CDCJ%282013%29Misc7E.pdf

72 United Nations, "General Comment No. 31 [80] Nature of the General Legal Obligation Imposed on States Parties to the Covenant: 05/26/2004. CCPR/C/21/Rev.1/Add.13. (General Comments)"
http://www.unhchr.ch/tbs/doc.nsf/0/58f5d4646e861359c1256ff600533f5f

73 The BBC, "Fugitive Edward Snowden trapped in Russia - Putin," http://www.bbc.co.uk/news/world-europe-23318475

## Conclusion

The Council of Europe has long served as a leader in human rights, and as such would be welcomed in efforts to expand and reinforce commitments to furthering Internet freedom. The revelations over the past few months have shown that this will be no easy task. And the stakes are high. Indeed, Edward Snowden's statement to the European Parliament is salient in this regard: "The surveillance of whole populations rather than individuals threatens to be the greatest human rights challenge of our time. The success of economies and developed nations relies increasingly on their creative output. And if that success is to continue we must remember that creativity is the product of curiosity, which in turn is the product of privacy."[74]

The authors look forward to working with the Council of Europe and its Member States to further the Internet freedom agenda and implement strong, comprehensive protections to ensure that internationally recognised human rights, including the right to private life, protection of personal data, and due process of law are upheld.

***

74 Statement from Edward Snowden to LIBE Committee of European Parliament (3 October 2013) http://www.informationclearinghouse.info/article36412.htm